Universidade Federal de Santa Catarina
Programa de Pós-Graduação em
Engenharia de Produção

Cesar de Souza Machado

GERENCIAMENTO DA SEGURANÇA DA INFORMAÇÃO EM SISTEMAS DE TELETRABALHO

Dissertação de Mestrado

Florianópolis
2002

Cesar de Souza Machado

GERENCIAMENTO DA SEGURANÇA DA INFORMAÇÃO EM SISTEMAS DE TELETRABALHO

Dissertação apresentada ao
Programa de Pós-Graduação em
Engenharia de Produção da
Universidade Federal de Santa Catarina
como requisito parcial para obtenção
do grau de Mestre em
Engenharia de Produção

Orientador: Roberto Carlos dos Santos Pacheco, PHD

Florianópolis
2002

FICHA CATALOGRÁFICA

Machado, Cesar de Souza
Gerenciamento da segurança da informação em sistemas de teletrabalho / Cesar de Souza Machado. – Florianópolis, 2002.
136 p. : il.

Dissertação (mestrado) – Universidade Federal de Santa Catarina, 2002.
Bibliografia.

1. Segurança da Informação 2. Processamento de Dados – Medidas de Segurança 3. Tecnologia da informação 4. Teletrabalho

CDU 004.056

Cesar de Souza Machado

GERENCIAMENTO DA SEGURANÇA DA INFORMAÇÃO EM SISTEMAS DE TELETRABALHO

Essa dissertação foi julgada e aprovada para a obtenção do grau de **Mestre em Engenharia de Produção no Programa de Pós-Graduação em Engenharia de Produção** da Universidade Federal de Santa Catarina

Florianópolis, 01 de abril de 2002.

Ricardo Miranda Barcia, PHD
Coordenador do Programa

BANCA EXAMINADORA

_____	_____
Andrea Valéria Steil	Roberto Carlos dos Santos Pacheco, Dr **Orientador**
_____	_____
Édis Mafra Lapolli, Dra	Elizabeth Sueli Specialski, Dra

Aos meus companheiros de jornada:
Denise, pelo apoio constante,
meus filhos Cesar Filho e Vitor.

Agradecimentos

À Universidade Federal de Santa Catarina.
À União Educacional de Brasília – UNEB
Ao orientador Prof. Roberto Carlos dos Santos Pacheco,
pelo acompanhamento pontual e competente.
Aos professores e colegas do PPGEP/UFSC.
A Cesar de Souza Machado Filho, Claudia de Souza Machado e Denise Nascimento Machado pelos trabalhos de revisão.
A Vicente Antonio de Avila pela ajuda no processamento estatístico dos dados.
A Maria Dalva Martins Palhano pelas sugestões para elaboração e validação do questionário de pesquisa.
A Profa. Andrea Valeria Steil, pela orientação e inestimável
auxílio, sem o qual não teria sido possível
a conclusão desse trabalho.

A todos os que direta ou indiretamente
contribuíram para a realização
desta pesquisa.

"Às vezes, quando considero as tremendas conseqüências advindas das pequenas coisas ... sou tentado a pensar ... não existem pequenas coisas."

Bruce Barton

Resumo

MACHADO, Cesar de Souza. **Gerenciamento da Segurança da Informação em Sistemas de Teletrabalho**. 2002. 136 f. Dissertação (Mestrado em Engenharia de Produção) - Programa de Pós-Graduação em Engenharia de Produção, UFSC, Florianópolis.

O presente trabalho apresenta um estudo sobre a segurança da informação em sistemas de teletrabalho. Faz-se uma incursão sobre o histórico e principais características do teletrabalho, mostrando suas relações com a segurança da informação, suas implicações e como esse tema foi abordado até o presente.

Com objetivo de subsidiar o gerenciamento da segurança da informação, uma pesquisa foi realizada para verificar como as empresas brasileiras estão administrando seus programas de teletrabalho com relação à segurança da informação. Com base na fundamentação teórico-empírica e nos resultados da pesquisa, foi estruturada uma metodologia baseada em um modelo de segurança para garantir a confidencialidade das informações em sistemas de teletrabalho. Partindo-se de um contexto de acesso remoto – uma atividade meio – o modelo delineado, implementado por meio de ferramentas e controles desenvolvidos a partir da norma ISO/IEC 17799, focaliza a atividade fim – a realização do teletrabalho.

Os resultados obtidos, por meio da aplicação do modelo em uma situação real, permitiram validar a aplicação da metodologia proposta como um instrumento efetivo para o gerenciamento da segurança das informações, atendendo de forma rápida e eficiente as necessidades de empresas e teletrabalhadores.

Palavras-chave: ISO/IEC 17799, modelo de segurança, segurança da informação, teletrabalho

Abstract

MACHADO, Cesar de Souza. **Gerenciamento da Segurança da Informação em Sistemas de Teletrabalho**. 2002. 136f. Dissertação (Mestrado em Engenharia de Produção) - Programa de Pós-Graduação em Engenharia de Produção, UFSC, Florianópolis.

The present work presents a study on the safety of the information in telework systems. An incursion is made on the report and principal characteristics of the telework, showing its relationships with the safety of the information, its implications and as that theme were approached until the present. With objective of subsidizing the administration of the safety of the information, a research was accomplished to verifying as the Brazilian companies are managing its telework programs with relationship the safety of the information. With base in the theoretical-empiric fundamentation and in the results of the research, a methodology was structured based on a model of safety to guarantee the confidenciality of the information in telework systems. Breaking of a context of remote access - an half activity - the delineated model, implemented through tools and controls developed starting from the norm ISO/IEC 17799, it focalizes the core activity - the accomplishment of the telework. The obtained results, through the application of the model in a real situation, allowed to validate the application of the methodology proposed as an effective instrument for the administration of the safety of the information, providing a fast and efficient way the needs of companies and teleworkers.

Key-words: information security, ISO/IEC 17799, security model, telework

Sumário

Lista de Figuras

Lista de Quadros

Lista de Tabelas

Lista de Abreviaturas e Siglas

ABNT	Associação Brasileira de Normas Técnicas
APR	Análise Preliminar de Riscos
CCSC	Commercial Computer Security Centre
COBIT	Control Objectives for Information and Related Technology
CORBA	Common Object Request Broker Architecture
DMZ	Demiliteried Zone
DSL	Digital Subscriber Line
E-Board	Electronic Board
E-MAIL	Electronic Mail
EUA	Estados Unidos da América
GUI	Graphic User Interface
ETO	European Telework Organization
FBI	Federal Bureau of Investigations
FTP	File Transfer Protocol
HTML	HyperText Markup Language
HTTP	Hypertext Transfer Protocol
IDS	Intrusion Detection System
IEC	International Electro-technical Commission
IIOP	Internet Inter-Orb Protocol
IMAP4	Internet Message Access Protocol version 4
IRC	Internet Relay Chat
ISACA	Information Systems Audit and Control Association
ISACF	Information Systems Audit and Control Foundation
ISDN	Integrated Service Digital Network
ISO	International Organization for Standardization
ISP	Internet Service Provider
LDAP	Lightweight Directory Access Protocol
MAN	Metropolitan Area Network
MIME	Multipurpose Internet Mail Extensions
NBR	Norma Brasileira

NC	Network Computer
NNTP	Network News Transfer Protocol
PKI	Public Key Infraestructure
PGP	Pretty Good Privacy
PKI	Public Key Infrastructure
POP3	Post Office Protocol version 3
RADIUS	Remote Authentication Dial-In User Service
RFC	Request For Comments
SMTP	Simple Mail Transfer Protocol
NNTP	Network News Transport Protocol
S/MIME	Secure Multipurpose Internet Mail Extensions
SSL	Secure Sockets Layer
TACACS	Terminal Access Controller Access Control System
TCP/IP	Transmission Control Protocol/Internet Protocol
TI	Tecnologia da Informação
VPN	Virtual Private Network
WWW	World Wide Web
X.509	Formato de certificado digital

1 INTRODUÇÃO

1.1 Origem e Evolução do Teletrabalho

Ao longo da história, à medida em que vêm evoluindo a tecnologia e as atividades humanas, o trabalho vem assumindo diferentes formas de expressão. Em termos históricos, predominaram inicialmente as atividades extrativistas, a caça e pesca, passando pelo horizonte agrícola e mais tarde pela revolução industrial.

Nas últimas décadas, o rápido desenvolvimento das Tecnologias de Informação (TI) vem possibilitando a flexibilização da forma como o homem trabalha, se organiza e interage socialmente (MUTSAERS, 1998).

O teletrabalho, proposto formalmente no início dos anos 70 (NILLES, 1996), surgiu como uma forma de flexibilização do trabalho (KUGELMASS, 1996), onde, através de recursos computacionais e de telecomunicações, o trabalhador pode executar suas atividades fora da sede da empresa, evitando o deslocamento até a mesma, o que, nos grandes centros urbanos, é causa de diversos problemas, como poluição do ar e congestionamentos de tráfego.

As condições para a disseminação da prática do teletrabalho surgiram nos anos 90, quando o aumento da concorrência e a sofisticação da demanda passaram a exigir respostas mais rápidas e maior flexibilidade em função das mudanças do mercado global (TEIXEIRA JUNIOR, 1999). Esses fatores proporcionaram o surgimento e popularização de tecnologias como a Internet, *notebooks* e computação móvel (DEIGHTON, 2000) tornando o teletrabalho possível a milhões de pessoas (TROPE, 1999).

Apesar da disponibilidade desses recursos, como constata Pliskin (1997), o teletrabalho ainda não obteve uma penetração substancial na sociedade, sendo alvo de constantes estudos e pesquisas por parte das organizações e pela comunidade acadêmica que tentam apreender toda a abrangência e implicações desse fenômeno.

Um dos motivos para esse fato está na questão da segurança das informações (KUGELMASS, 1996), ou seja, a mesma base tecnológica que possibilitou o surgimento e que hoje viabiliza o teletrabalho, pode ser a fonte de

inúmeros problemas na medida em que aumentam os riscos para a integridade, confidencialidade e disponibilidade das informações necessárias à manutenção das organizações. Tal fato se justifica na medida em que a informação assumiu importância vital para manutenção dos negócios nos dias atuais, marcados pela dinamicidade da economia globalizada e permanentemente *on-line*, de tal forma que o comprometimento do sistema de informações por problemas de segurança pode causar grandes prejuízos ou mesmo levar a organização à falência (CARUSO, 1999). Foi com objetivo de proteger as informações e garantir a continuidade dos negócios que, em 2000, foram homologadas as normas de segurança da informação BS7799, na Inglaterra, e a norma internacional ISO/IEC 17799.

No universo das empresas, encontra-se uma diversidade de casos, tal como organizações que implementam o teletrabalho sem medidas de segurança das informações, outras que implementam medidas insuficientes e ainda aquelas que, diante dos riscos e ameaças envolvidos, optam por não empregar teletrabalhadores para não facilitar o acesso a informações sensíveis (STURGEON, 1996).

Dessa forma, com a finalidade de descrever e equacionar satisfatoriamente essa questão, viabilizando a implantação e gerenciamento de sistemas de teletrabalho, esse estudo se pauta pela seguinte pergunta de pesquisa:

“Como gerenciar a segurança da informação em sistemas de teletrabalho?”

1.2 Objetivos geral e específicos

1.2.1 Objetivo Geral

Esta dissertação possui como objetivo geral propor uma metodologia para gerenciamento da segurança da informação em sistemas de teletrabalho, que contemple os controles previstos pelas normas de segurança da informação BS7799, ISO/IEC 17799 e NBR ISO/IEC 17799.

1.2.2 Objetivos Específicos

Em termos específicos, procurou-se alcançar os seguintes objetivos:

- Apresentar as relações teóricas e empíricas entre segurança da informação e teletrabalho;
- Analisar como as organizações brasileiras que realizam o teletrabalho estão tratando a questão da segurança das informações e
- Propor uma metodologia para o gerenciamento da segurança das informações para estas organizações.

1.3 Justificativa Teórica e Prática

O *Teletrabalho*, segundo a *European Telework Organization* (2001), ocorre quando tecnologias de informação e comunicação são aplicadas para possibilitar a realização do trabalho à distância do local onde o resultado do trabalho é necessário ou onde o trabalho poderia ser feito da forma convencional. Essa definição aplica-se a teletrabalhadores baseados em suas residências, teletrabalhadores móveis, e teletrabalhadores baseados em centros de teleserviço.

Segundo a norma ISO/IEC 17799:2000, *Segurança da Informação* pode ser definida como a proteção contra um grande número de ameaças às informações, de forma a assegurar a continuidade do negócio, minimizando danos comerciais e maximizando o retorno de investimentos e oportunidades. Ainda segundo a ISO/IEC 17799:2000 a segurança da informação é caracterizada pela preservação dos três atributos básicos da informação: c*onfidencialidade, integridade e* d*isponibilidade.*

Problemas com a segurança das informações, conforme Caruso (1999), podem causar grandes prejuízos à empresa, que tanto podem ser financeiros como podem afetar sua imagem, podendo inclusive, em certos casos, levá-la à falência. A falta de segurança, como afirma Kugelmass (1996) é um dos motivos pelos quais as empresas podem desestimular a adoção do teletrabalho.

Autores como Nilles (1997), Trope (1999), Mello (1999) e Leonhard (1995) abordam a questão da segurança das informações no teletrabalho de forma

superficial; outros como Moustafa (2000), Yasin (2000) e Connor (2000), exploram questões pontuais quanto à segurança da informação aplicáveis ao teletrabalho, de forma que a implantação e gerenciamento da segurança da informação nesses sistemas, quando muito, poderão ser baseados em *checklists* disponíveis na Internet, tal como no do *Smart Valley Telecommuting Guide* (1998), disponibilizado na Internet pela Cisco Systems.

A relevância dessa pesquisa está na contribuição para proporcionar um entendimento adequado da relação teletrabalho e segurança da informação, propondo uma metodologia para gerenciamento da informação em sistemas de teletrabalho baseada nos controles previstos pelas normas de segurança da informação BS7799 e ISO/IEC 17799, publicadas em 2000, e na norma NBR ISO/IEC 17799, publicada em 2001.

Em termos práticos, os resultados dessa pesquisa poderão oferecer subsídios para a viabilização da implantação e gerenciamento do teletrabalho.

1.4 Estrutura da Dissertação

Este trabalho foi estruturado em 6 capítulos, a saber: no primeiro capítulo apresenta-se uma visão geral do teletrabalho e da segurança da informação, fatores geradores da pergunta de pesquisa investigada, além da apresentação dos objetivos geral e específicos.

O segundo capítulo refere-se à fundamentação teórico-empírica que é a base para a presente pesquisa na qual se procura evidenciar os conceitos e características do teletrabalho e da segurança da informação, apresentando uma revisão bibliográfica referente à relação entre esses temas apontando suas correlações.

O terceiro capítulo apresenta a metodologia usada nesse estudo, destacando as perguntas de pesquisa, as definições das variáveis, delimitação da pesquisa, técnicas de coleta de dados e as limitações associadas a essa pesquisa.

O quarto capítulo contém a apresentação e a análise dos dados coletados na pesquisa conforme o referencial metodológico apresentado no capítulo terceiro, tendo por base a fundamentação teórico-empírica abordada no segundo capítulo desse trabalho.

O quinto capítulo apresenta um modelo de segurança com finalidade de assegurar a integridade, disponibilidade e confidencialidade das informações em sistemas de teletrabalho.

O sexto e último capítulo apresenta, por fim, as conclusões do trabalho e recomendações observadas.

Finalmente, são apresentadas as referências bibliográficas e os anexos.

2 FUNDAMENTAÇÃO TEÓRICO EMPÍRICA

Nesse capítulo são caracterizados o teletrabalho e a segurança da informação, sendo apresentadas suas principais características e uma revisão bibliográfica sobre como as correlações entre esses dois temas foram abordadas até o presente momento.

2.1 Evolução das Atividades Humanas

Na idade média o trabalho era exercido quase sempre com a terra, envolvendo o cultivo de grãos e a criação de gado para extração de leite, lã ou carne. A unidade industrial típica da idade média era uma pequena oficina, tendo um mestre como empregador trabalhando lado a lado com seus ajudantes (HUBERMAN,1979).

Lentamente, os trabalhadores foram se organizando, de forma que, com o tempo, surgiram as corporações de trabalhadores artesanais que exerciam o controle das atividades produtivas e comerciais. Segundo Huberman (1979), essas corporações passaram a monopolizar o comércio na idade medieval e assim o fizeram até o início da revolução industrial, sendo definitivamente abolidas no início do século XIX.

A invenção de máquinas para fazer o trabalho do homem é algo muito antigo. Como Huberman (1979) descreve, no fim do século XVIII, contudo, a associação da máquina a vapor provocou uma modificação importante no método de produção. Com a revolução industrial, surgiu na Inglaterra o sistema fabril de larga escala que modificou profundamente a economia, possibilitando uma redução de até 1000 % nos preços dos produtos (DRUKER, 1999), que passaram a atingir um mercado consumidor muito maior. Nesse cenário surgiu um novo tipo de trabalhador – o operário industrial.

No final do século XIX, ocorreu uma segunda revolução industrial (CASTELS 2001). Esta baseou-se em novos conhecimentos científicos, tais como o uso da eletricidade e do motor de combustão interna (Estados Unidos) e na industrialização de produtos químicos com bases científicas (Alemanha).

No início do século XX, teóricos como Taylor e Fayol constituíram as bases para uma administração científica da produção, possibilitando enormes ganhos na produtividade dos trabalhadores (CHIAVENATO, 1987). Suas teorias coincidiram com o advento da primeira guerra mundial que, segundo Druker (1999), evidenciou a necessidade de uma estrutura organizacional clara, até então inexistente.

Conforme salienta Nilles (1997), da primeira revolução industrial até a década de 1950, a indústria foi a principal fonte de empregos e de produção de PIB em todos os países. A partir da década de 50, no entanto, o desenvolvimento científico e tecnológico tornou-se muito acelerado, em grande parte devido à "Guerra Fria", proporcionando o desenvolvimento dos primeiros computadores e redes de comunicação de dados, tal como a Internet, criada em 1969 nos Estados Unidos.

Na década de 70, as novas tecnologias de informação se difundiram amplamente, acelerando seu desenvolvimento sinergético e convergindo em um novo paradigma tecnológico (CASTELS, 2000).

Toffler (1995), analisando esse novo paradigma, identificou três revoluções ou ondas ao longo da história, cada uma delas evoluindo paralelamente e coexistindo entre si:

- A Primeira onda - a agrícola
- A Segunda onda - a industrial
- A Terceira onda - a informação

Conforme Druker (1999) salienta, a era que ora se consolida, passou a ser denominada a "Era da Informação", consistindo em uma revolução de conceitos e não de técnicas ou ferramentas, trazendo consigo profundas mudanças estruturais em nossa sociedade.

Segundo Trope (1999), na sociedade da era da informação, as novas tecnologias influenciam cada vez mais o modo como nos organizamos, administramos e definimos as regras para as empresas. Dentro deste contexto, a tendência predominante assinala que a maior parte do trabalho tende a ser realizado em função da obtenção ou do tratamento das informações.

De acordo com o referido autor, às rápidas e bruscas mudanças atuais, a forte competição entre as empresas e a globalização da economia são fatores que, entre outros, fazem com que as organizações tenham de lidar não mais com a

previsibilidade, a continuidade e a estabilidade, mas sim com seus contrários, ou seja, com a incerteza.

A flexibilidade passou a ser então uma necessidade para as organizações. A diminuição das fronteiras intra e interorganizacionais passou a gerar novas formas organizacionais, caracterizadas pela dispersão temporal e espacial (STEIL e BARCIA, 2001). Nesse contexto surgiu e tem se desenvolvido a proposta do teletrabalho.

2.2 Teletrabalho

2.2.1 Surgimento do Teletrabalho

Jack Nilles propôs nos Estados Unidos o conceito de Teletrabalho a partir de seu trabalho junto à NASA, em 1970, e, posteriormente, na Fundação Nacional de Ciências em 1973 (NILLES, 1996).

Nilles começou a construir o conceito de teletrabalho (o qual denominou inicialmente *telecommuting)* com objetivo de criar uma alternativa aos longos deslocamentos aos quais tinham de se submeter os trabalhadores dos grandes centros urbanos dos Estados Unidos da América para ir ao trabalho e retornar dele, num processo denominado *commuting*, responsável por um grande gasto de tempo (ANDREASSI, 1997; REYMERS, 1998) além de contribuir para com o agravamento da poluição e com o gasto de combustíveis (NILLES, 1996).

A proposta de Nilles (1997) era que os trabalhadores poderiam exercer suas atividades em seus domicílios, o que em si não era uma novidade, mas empregando recursos de computação e de telecomunicações, o que consistia em um novo paradigma nas relações de trabalho: o “Teletrabalho no Domicílio” (VERAS OLIVEIRA, 1996), onde o contato entre as pessoas ocorre também por meios eletrônicos de comunicação.

Nilles publicou suas conclusões em 1976 no livro "The Telecommunications Transportation Trade-Off" quando propôs o termo *Telecommuting* que, em português, tem como similar mais próximo o termo “Teletrabalho” (MELLO, 1999).

Embora o teletrabalho possa parecer novo, não se trata de um estilo de trabalho sem precedentes. Experiências precursoras de teletrabalho foram realizadas em 1962 na Inglaterra (STEIL e BARCIA, 2001). Kugelmas (1996) cita que iniciativas nesse sentido remontam à 1857, quando uma estrada de ferro nos Estados Unidos empregou o telégrafo para gerenciar funcionários localizados em um escritório distante.

O teletrabalho se tornou possível devido ao grande desenvolvimento ocorrido nos setores de telecomunicações e informática. O surgimento e popularização dos computadores pessoais na década de 80 marcou o início da informatização do local de trabalho (BELL, 2000). Na década de 90, o aperfeiçoamento dos computadores pessoais, o surgimento das interfaces gráficas como Windows e Motif puseram a TI ao alcance de centenas de milhões de pessoas, criando a base tecnológica para a popularização do teletrabalho (CASTELS, 2000).

Ao longo da década de 80, diversos trabalhos e pesquisas foram desenvolvidos nos Estados Unidos e Europa, tais como os de Olson, (Citado por THOMPSON, 1998) Miles e Sonw (Citados por PLISKIN, 1997) Shamir e Salomon, Beer e Blanc (Citados por VERAS OLIVEIRA, 1996), visando delinear as características e impactos do teletrabalho nas atividades das empresas e na economia, bem como testar as premissas e propostas de Nilles.

Em alguns países, como nos Estados Unidos, o governo incentivou as empresas a adotarem o Teletrabalho como uma alternativa para redução da poluição do ar (REYMERS, 1998). Nem todos, contudo, receberam bem essas propostas. Na Europa, sindicatos de trabalhadores reagiram contra o teletrabalho por considerarem que ele, dentre outros motivos, provocaria a desunião dos funcionários das empresas (MELLO, 1999).

Em um sentido mais amplo, o teletrabalho surgiu e vem se desenvolvendo em meio a um acelerado processo de abertura de fronteiras e barreiras comerciais, fenômeno que, nos anos 90, foi cunhado como “globalização”. Alvo de grandes controvérsias, a globalização poderá vir a subverter as tradicionais estruturas de estado e poder, devido à circulação instantânea de informações, trabalho e divisas, todas de controle difícil .

Bell (2000) sintetiza em um quadro a evolução do espaço de trabalho que começa com as organizações tradicionais e centralizadas, passa pela adoção da TI,

dividida em duas fases – a informatização e a interligação em redes, até chegar na fase da virtualização das empresas, nos dias atuais e no futuro próximo (Figura 2.1).

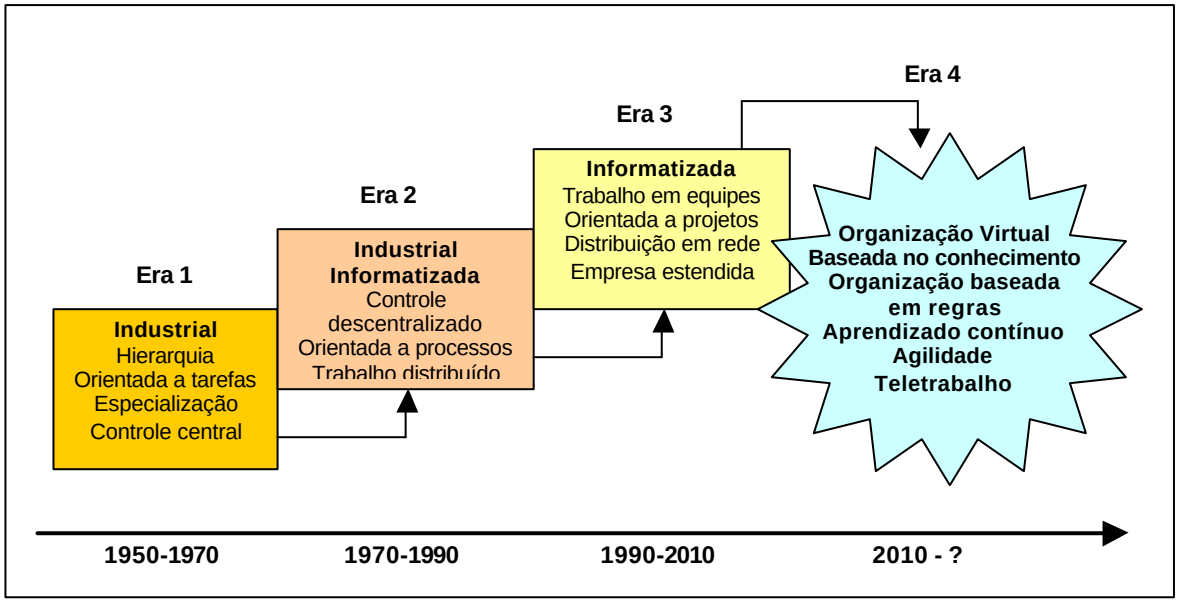

Figura 2.1: As Quatro Fases da Evolução do Espaço de Trabalho

Fonte: Adaptado do Gartner Groups, 1999

2.2.2 Teletrabalho Hoje

Hoje, para sobreviver num ambiente turbulento e de crescente competitividade, as organizações estão buscando alternativas viáveis para seus negócios, assim como estruturas organizacionais e novas formas de trabalho. A partir dessa perspectiva, várias formas de flexibilização do trabalho vêm sendo criadas. Nesse contexto, o teletrabalho surge como uma alternativa moderna de gestão empresarial (MELLO, 1999), sendo empregado, mais recentemente, em certos casos, como uma forma de atrair e reter o funcionário na empresa (KURLAND, 1999).

O desenvolvimento das tecnologias de informática e telecomunicações impactaram de tal forma a estrutura e dinâmica das organizações que se tornou possível a criação de organizações virtuais, capazes de operar em ritmos, velocidades ou qualidades de história diferentes das organizações convencionais (LÉVY, 1996).

Presentes para seus clientes somente no ciberespaço da Internet, as organizações virtualizadas são caracterizadas, segundo Lévy (1996), pela *desterritorialização* e pelo *efeito Moebios*, ou seja, a passagem do interno para o externo e do externo para o interno, onde o teletrabalho é um processo de arranjo intrínseco (ANDREASSI, 1997).

O teletrabalho apresenta diversas vantagens potenciais de tal forma que, muitas vezes, é considerado uma panacéia para os empregados (KURLAND, 1999). Contudo, apesar de suas vantagens, o teletrabalhador freqüentemente é confundido por seus familiares como "aquele que levou algum trabalho para fazer em casa". Esse tipo de reação negativa, fruto do condicionamento cultural, poderá gerar atritos familiares que podem causar o fracasso da iniciativa de se retirar o trabalhador do escritório (JAMIL, 2001).

Segundo Jamil (2001), embora o teletrabalho seja uma forma versátil e flexível de produzir na nova ordem econômica, ele ainda é mal compreendido e mal usado. Para este autor, a promessa de se estar diante de uma nova empresa, de se ter maior agilidade, menor hierarquia e maior flexibilidade, tratando o empregado com maior confiança, é hoje uma dura prova para o teletrabalho.

A visão de Jamil é corroborada por outros autores, como Pliskin (1997), que vê um paradoxo no fato de, apesar de toda a tecnologia da informação necessária ao teletrabalho já estar disponibilizada, sua adoção ainda está muito abaixo das possibilidades e expectativas.

Kugelmass (1996) sugere que isto ocorre pela visão administrativa atual ainda atrelada à tradição. Reymers (1998) assinala que o fato do teletrabalho ser um tema relativamente novo, faz com que alguns pesquisadores tendam a encará-lo mais como um constructo ideológico do que uma realidade metodológica.

Numerosas pesquisas indicam que o número de teletrabalhadores está aumentando (KUNDU, 1999), contudo, como demonstra Reymers (1998), as diversas pesquisas realizadas nos Estados Unidos apontam números muito diferentes de teletrabalhadores. Segundo Sparrow (2000), as estimativas sobre o número de pessoas envolvidas com teletrabalho variam conforme o tipo de pesquisa realizada e as definições de teletrabalho empregadas. Segundo o Telework America 2000, o número de teletrabalhadores nos EUA no ano 2000 seria de 23,6 milhões, com um crescimento da ordem de 20,6% com relação a 1999. Segundo Kundu (1999), as estatísticas levam em conta diversos tipos de teletrabalhadores, inclusive

aqueles que não possuem computadores, o que, pela definição da ETO, adotada nessa dissertação, não caracterizaria os mesmos como teletrabalhadores de fato, razão pela qual se pode projetar um número de teletrabalhadores nos Estados Unidos menor do que os apresentados nas pesquisas.

Na Europa, segundo o *Status Report on European Telework – "Telework 1999"*, também houve um rápido crescimento no número de teletrabalhadores nos últimos anos, registrando-se 1,5, 2 e 2,9 milhões de teletrabalhadores formais em 1997, 1998 e 1999, respectivamente. Segundo este relatório, se forem considerados os teletrabalhadores informais, eventuais e autônomos, seu número chegaria a 9,0 milhões em 1999. Apesar desse crescimento, os teletrabalhadores formais correspondiam a 1,6% da força de trabalho européia em 1999.

Trope (1999) questiona se o advento do teletrabalho marcaria o desaparecimento do Taylorismo e, por conseguinte, o fim do atual modelo de organização. O referido autor também aponta o teletrabalho como uma ferramenta de globalização, na medida em que permite às empresas utilizarem mão-de-obra de qualquer parte do mundo.

Permitindo ao homem dominar o trabalho em termos de tempo e lugar, o teletrabalho provoca muitos impactos nas organizações, os quais, ainda estão sendo estudados sob diversos pontos de vista: tecnológicos (DAVIES, 1996) jurídicos (ZABROSKY, 2000), econômicos (KURLAND, 1999), sociais (REYMERS, 1998) e psicológicos (MAN, 2000).

Por outro lado, nada impede que, pressionados por questões tais como a poluição, gastos de combustíveis e congestionamento de tráfego, os governos no futuro venham a incrementar o teletrabalho através da implementação de políticas sociais e econômicas (REYMERS, 1998).

2.2.3 Definição de Teletrabalho

O teletrabalho tem recebido diversas denominações tais como *telework, telecommuting, electronic homework, electronic cottage, networking*, "trabalho a distância", "trabalho independente do local", dentre outras (REYMERS, 1998), nem sempre aceitas ou compartilhadas por pesquisadores da área (DAVIES, 1996).

Segundo Reymers, tal diversidade pode ser explicada pela forma como são interpretadas as diferentes formas de se trabalhar fora da empresa.

Para Nilles (1996), *Telework* é uma forma de trabalho descentralizado, uma atividade periódica fora do escritório central, um ou mais dias por semana, seja em casa ou em um centro de teleserviço, através de recursos de telecomunicações e/ou informática.

Uma comissão francesa de estudo sobre o teletrabalho delineou uma definição com finalidade jurídica: *Teletrabalho é uma modalidade de organização e execução de um trabalho exercido a título habitual, por uma pessoa física, com as seguintes condições cumulativas: a distância; sem supervisão da execução por parte do solicitante; através do uso de ferramentas de informática e telecomunicações* (TROPE, 1999).

Telecommuting é um termo que está relacionado à substituição dos meios de transporte, que levam o indivíduo até o trabalho, pelos meios de comunicação de dados, que levam o trabalho até o indivíduo (VERAS OLIVEIRA, 1996).

Com relação à utilização regional dos termos, o *telecommuting,* criado por Nilles, é mais empregado nos Estados Unidos, ao passo que *telework* é mais empregado e difundido na Europa. O termo *telework,* por ser um conceito mais amplo, onde "tele" significa "ao longe" (FERREIRA, 1986) e "work" significa "trabalho" (MICHAELLIS, 1987) tem sido considerado mais adequado do que o *telecommuting, onde* "commuting" significa viajar diariamente de casa para o trabalho (NILLES, 1996), sendo esse último um dos tipos ou subconjuntos do *telework* (Figura 2.2). No Brasil e em Portugal emprega-se o termo Teletrabalho, uma tradução direta para o português de *telework*. Todos os termos têm em comum o fato de se referirem à idéia de que o trabalhador encontra-se fora da empresa.

Nessa pesquisa, será adotada a definição de teletrabalho, proposta pela *European Telework Organization* (2001), segundo a qual, o "teletrabalho é geralmente interpretado como "teletrabalho baseado em casa" com uso de computadores e telecomunicações, apresentando-se sob várias formas e características". Ainda segundo a ETO, o "teletrabalho ocorre quando tecnologias de informação e comunicação são aplicadas para possibilitar a realização do trabalho à distância do local onde o resultado do trabalho é necessário ou onde o trabalho poderia ser feito da forma convencional".

Essa definição aplica-se a teletrabalhadores baseados em suas residências, teletrabalhadores móveis, e teletrabalhadores baseados em centros de teleserviço.

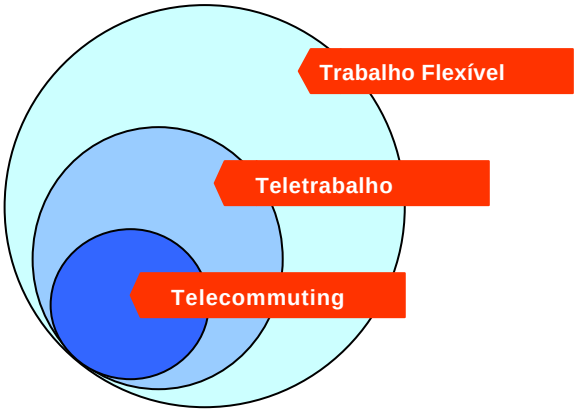

Figura 2.2: Trabalho Flexível, Teletrabalho e Telecommuting

2.2.4 Classificação dos Teletrabalhadores no Domicílio

Segundo a European Telework On Line (2001), os teletrabalhadores baseados em seus domicílios podem ser classificados em quatro categorias:

1) **Teletrabalhador empregado:** funcionário da organização formalmente contratado por tempo indeterminado, possui todas as garantias e benefícios inerentes ao trabalho legalizado.
2) **Autônomo ou Freelancer:** funcionário temporário que atende as necessidades do mercado, podendo teletrabalhar para a organização baseado em um contrato de prestação de serviços.

3) **Informal:** funcionário que atua como teletrabalhador sem que essa condição seja formalizada ou legalmente reconhecida pela organização.

4) **Empreendedores:** pessoas que montam seu primeiro negócio em casa, antes de abrirem seu primeiro escritório ou empresa formal.

O teletrabalho não é uma atividade tipicamente de tempo integral. Segundo Dunning (1997), em muitas organizações o teletrabalhador vai regularmente à empresa para participar de reuniões, ou trabalhar de forma convencional, onde pode manter um contato face a face com outras pessoas, um tipo de comunicação considerada essencial por muitos profissionais. Conforme esse autor salienta, o entusiasmo de um aperto de mão não pode ser sentido através do teletrabalho, mesmo empregando-se teleconferência.

É importante ressaltar que, independente de suas atividades como teletrabalhador, o funcionário de uma empresa pode vir a exercer outras atividades profissionais ou sociais não relacionadas à sua atividade principal.

Fisicamente, o teletrabalhador pode se situar em inúmeras localidades ou condições, tais como escritórios satélites, filiais ou agências da organização, centros de teleserviço, em trânsito (em aviões, embarcações, trens), nas instalações do cliente, em campo e, por fim, em sua residência. Apesar dessa diversidade de localizações, segundo Nillles (1997), o funcionário localizado em sua residência representa o padrão do teletrabalho.

Com relação à distribuição geográfica, os teletrabalhadores podem estar localizados, com relação a sede da organização, na mesma cidade, estado, país ou ainda em outros países, uma vez que as telecomunicações tornam a distância praticamente irrelevante.

2.2.5 Tipos de Atividades

Teletrabalhadores podem exercer as mais variadas atividades relacionadas à empresa, especialmente as mais ligadas à produção intelectual, tal como engenharia, arquitetura e desenvolvimento de *software*. Segundo Schill (1999), os setores comercial e governamental podem ser especialmente beneficiados pela descentralização de serviços de valor-agregado em áreas rurais, particularmente nas áreas de comunicação, engenharia, serviços comerciais, consultoria, *design* gráfico, editoração e mídia, serviços financeiros, serviços administrativos sub-contratados e serviços de secretaria e transporte. Segundo Soares (1995), essas atividades seriam um pólo das qualificações dos teletrabalhadores, sendo o outro formado por tarefas menos qualificadas, como digitação e processamento de textos.

Em um trabalho para a Administração Municipal de Los Angeles, Nilles (1997) relacionou 400 classificações e 16.000 funções que podem ser executadas por meio do teletrabalho. Este autor também cita o fato que, em 1990, 57% da mão de obra americana estavam alocadas nas áreas ligadas à comunicação e conhecimento, sendo razoável acreditar que no futuro esse percentual deva crescer, assim como a utilização de recursos tecnológicos cada vez mais sofisticados, proporcionando novas oportunidades para a prática do teletrabalho.

Segundo Dunning (1997), os teletrabalhadores normalmente são encontrados em empresas que possuem grande número de funcionários, de tal forma que elas podem distribuí-los entre a empresa e o trabalho a distância. Por outro lado, ainda segundo Dunning, pequenas empresas têm grande flexibilidade em sua estrutura, de forma que podem se adaptar rapidamente a mudanças nos sistemas de gerenciamento do trabalho.

2.2.6 Perfil do teletrabalhador

O perfil do teletrabalhador varia muito com relação às variáveis sexo, idade, formação, profissão, condição social e cultural (MELLO, 1999; TROPE, 1999).

A adequação de uma política de teletrabalho depende muito dos teletrabalhadores, que devem ter certas características psicológicas (DUNNING, 1997).

A utilização de testes psicológicos durante o recrutamento do teletrabalhador é recomendada por Gauthier e Dorin (Apud TROPE, 1999) como forma de determinação da adaptabilidade destes ao teletrabalho.

Segundo Nilles (1997), o “teletrabalhador ideal” deveria apresentar as seguintes características fundamentais: auto-motivação, autodisciplina, conhecimentos específicos e experiência profissional, flexibilidade e criatividade, facilidade em manter contatos sociais, estar na fase de vida adequada, estar com uma situação familiar estável e não necessitar de supervisão direta.

Steil e Barcia (2001), citando Bredin (1996) relacionam ainda como características desejáveis do teletrabalhador: saber administrar o tempo, lidar com desafios, resistir a distrações, comunicar-se eficazmente, obter motivação e criar e manter um equilíbrio adequado entre a vida profissional e particular.

Segundo Trope (1999), estudos psicológicos com teletrabalhadores demonstraram que eles não eram mais autônomos ou organizados, nem menos sociáveis do que os não-teletrabalhadores, levando a crer que sua única diferença, para estes, seria na sua vontade de teletrabalhar.

Contudo, apesar de importante, a vontade não se configura no único elemento importante. Segundo Nilles (1997), nem todas as pessoas podem ser bons teletrabalhadores. Esse autor propõe um processo de seleção dividido em duas partes: exame do conteúdo das funções e a avaliação dos aspectos psicológico/comportamentais do candidato a teletrabalhador.

O teletrabalho exige ainda um certo nível de escolaridade e conhecimentos de informática, assim como um grau de profissionalismo, qualificação e treinamento maior que os exigidos para a realização de trabalhos do domicílio em geral (VERAS OLIVEIRA, 1996), mas não necessariamente maiores do que os utilizados na empresa (STEIL e BARCIA, 2001; SCHILL, 1999).

Autores como Kugelmass (1996) descrevem uma análise da comutabilidade composta por um questionário envolvendo a natureza das tarefas envolvidas no trabalho do empregado. Por meio de formulários, os teletrabalhadores potenciais assinalam as tarefas que poderiam ser executadas a distância. Leva-se em consideração, ainda, o grau de desempenho de certas funções na empresa pelos teletrabalhadores potenciais. Com base nas respostas, pode-se verificar o grau de adequação do funcionário ao perfil do teletrabalhador.

Segundo Steil e Barcia (2001), o conhecimento aprofundado da função e a internalização dos aspectos mais importantes da cultura organizacional facilitam a adoção do teletrabalho, na medida em que contribuem para a manutenção de um conjunto de atitudes favoráveis à organização e ao estabelecimento de um contrato psicológico de trabalho.

Por fim, Nilles (1997) assinala como de fundamental importância o fato de o empregado ser sempre voluntário para teletrabalhar, de forma que a iniciativa do teletrabalho possa ser bem sucedida.

2.2.7 Ambiente do Teletrabalhador

O teletrabalhador pode se situar em sua residência ou deslocar-se para centros de teleserviços (telecentros), que podem ser mantidos pela empresa, por uma comunidade em áreas rurais (telecottages), por particulares (televillage), ou prestadores de serviços (escritórios virtuais). O teletrabalhador pode ainda ser um nômade, tal como um executivo que viaja constantemente e teletrabalha com seu *notebook* (ETO,2001). Na maior parte dos casos, como descrito anteriormente, o teletrabalhador situa-se em sua residência, razão pela qual essa dissertação focaliza o ambiente do teletrabalhador no lar.

A literatura aponta que no ambiente do teletrabalhador devem ser considerados os aspectos relacionados à adequação da execução do trabalho e, no caso do teletrabalho no lar, as rotinas domésticas que devem ser organizadas de tal forma que não ofereçam estímulos contrários à execução de suas atividades profissionais (STEIL e BARCIA, 2000).

Entretanto, nos postos de trabalho domiciliares, não é comum a preocupação com a ergonomia, *design* e aproveitamento racional do espaço, pois o interesse do trabalhador é primeiramente reduzir os custos operacionais, que nem sempre são pagos pela empresa. A aplicação dos princípios ergonométricos e macroergonométricos podem proporcionar, através da otimização do ambiente de trabalho, o aumento da produtividade e reduzir eventuais despesas indenizatórias ou tratamentos de saúde com funcionários (VERAS OLIVEIRA, 1996). Dessa forma, ajustes no ambiente quase sempre serão necessários para adequar o ambiente doméstico às necessidades do teletrabalhador.

Nesse sentido, Nilles (1997) recomenda um local permanente na casa destinado às atividades do teletrabalhador e uma inspeção do mesmo para verificar sua adequação, de forma que o escritório do teletrabalhador não represente mais riscos que o escritório, reduzindo assim a responsabilidade da empresa. O referido autor recomenda que o ideal é reservar uma área de 15 metros quadrados em média para constituir o escritório do teletrabalhador. Em certos locais, contudo, como nos grandes centros urbanos, tal disponibilidade de espaço pode ser inexeqüível.

Nilles (1997) recomenda ainda que o escritório do teletrabalhador deve atender as seguintes características: espaço de trabalho adequado, acesso a

tomadas elétricas e telefônicas, materiais de trabalho de acordo com as normas de segurança, isolamento acústico, distinção das atividades domésticas corriqueiras, controle de temperatura e iluminação, atenção para a ergonomia.

2.2.8 Telecomunicações

O acesso remoto, ou seja, a comunicação entre o teletrabalhador e a organização, é feita através de um modem (modulador/demodulador) ou um dispositivo de rede que possa converter os sinais digitais de dados do computador do teletrabalhador em um sinal analógico ou em um sinal digital banda base capaz de ser transmitido por um dos inúmeros meios ou serviços de comunicação de dados hoje disponíveis (BEHAMOU, 1998; CISCO, 1999; SCHILL,1999):

- Dispositivo de acesso a satélite
- Linha comutada (linha telefônica convencional)
- Linha privativa (*Leased Line*)
- ISDN (Integrated Services Digital Network)
- DSL (Digital Subscriber Line)
- *Cable Modem*
- *Frame Relay*
- Microondas (Wireless)
- Telefonia móvel (Mobile computing)
- Serviços T1 e T3 (Disponíveis nos Estados Unidos da América)
- Rede metropolitana – MAN
- Conexão com a Internet II

A escolha do serviço de telecomunicações é feita levando-se em conta o volume de tráfego demandado pelo teletrabalhador, os custos do serviço e a disponibilidade do mesmo na vizinhança do teletrabalhador.

O teletrabalho pode ser realizado *on line* ou *off line*, conforme representado na figura 2.3 , mas, em todo caso, a comunicação com a empresa terá de ser efetuada. No trabalho *on line*, é preciso efetuar e manter uma conexão entre o computador do teletrabalhador e o da empresa para se obter o acesso ao sistema

de informação da empresa. No sistema *off line* o teletrabalhador pode executar suas tarefas e enviá-las para a empresa por *e-mail* ou FTP onde serão posteriormente processadas conforme a disponibilidade ou o agendamento do sistema.

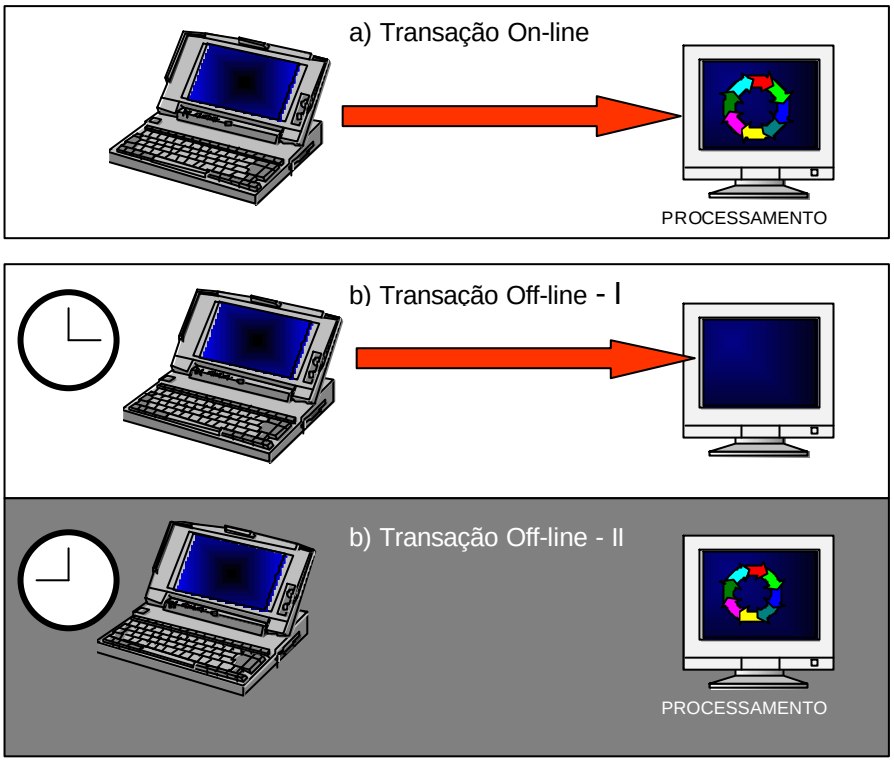

Figura 2.3: Sistemas On-line e Off-line

Segundo Shill (1999) as soluções, envolvendo *hardware*, *software* e telecomunicações para atender aos diversos tipos de teletrabalho podem ser divididas em três tipos, conforme apresentado na Figura 2.4.

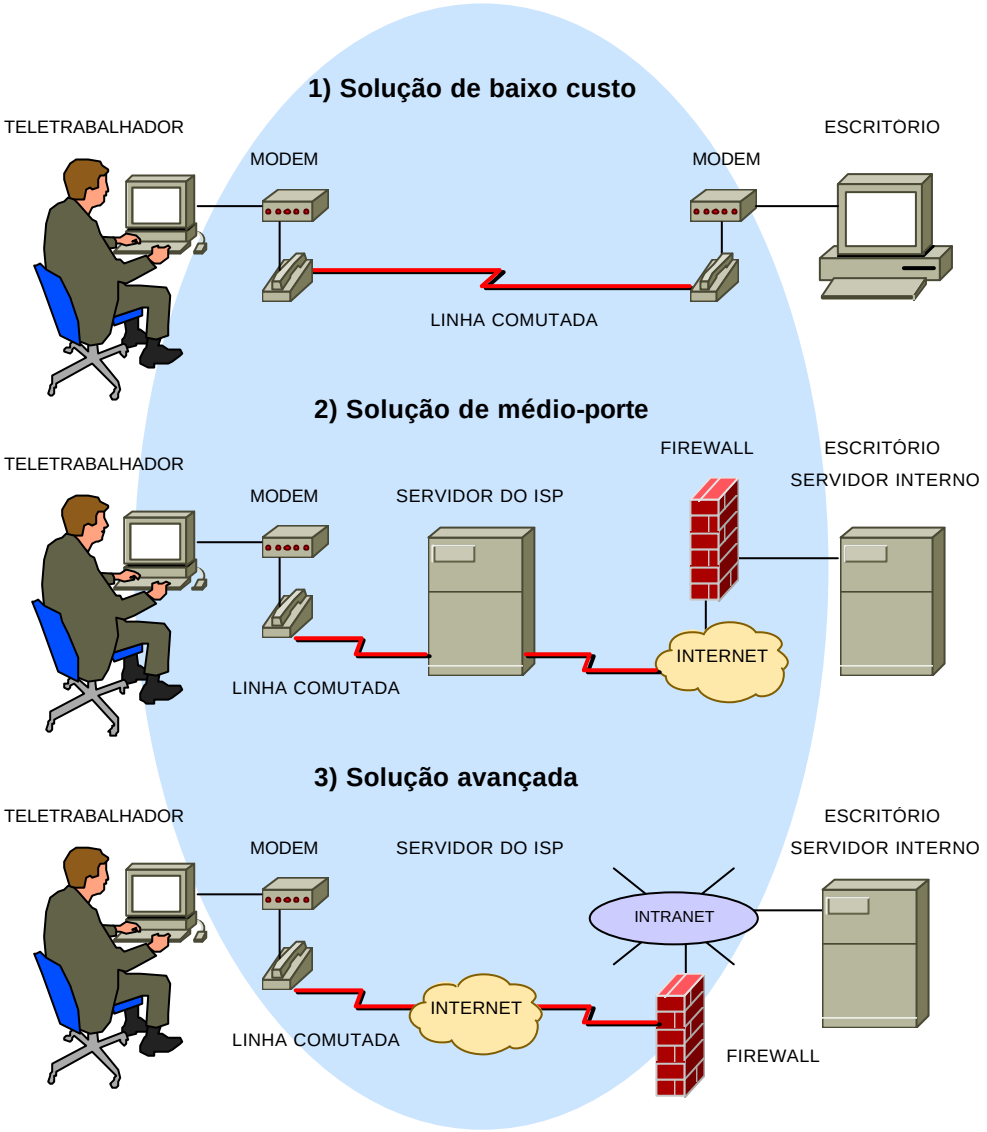

Figura 2.4: Soluções de Teletrabalho

Fonte: SHILL, 1999.

(1) **Solução de baixo custo:** utilizada para atividades mais simples de teletrabalho envolvendo a confecção de documentos e gravação de dados, empregando linhas telefônicas e telefax. Apenas a transferência dos documentos produzidos requer serviços de telemática.

(2) **Solução de médio-porte:** necessita uma conexão com a Internet e serviços WWW, E-mail e FTP para acesso a um servidor em um ISP (Internet Service Provider) através do qual o teletrabalhador trocará dados com a empresa.

(3) **Solução avançada:** para usuários experientes, envolve a utilização de todos os recursos da intranet da empresa e execução de tarefas complexas.

Essa classificação não é rígida, na medida em que o ambiente dos teletrabalhadores e das empresas são muito variados, comportando diversos tipos de configuração, conforme suas necessidades e disponibilidade de recursos.

A Cisco Networks (2001) recomenda a observação dos seguintes aspectos na escolha da melhor solução para sistemas de teletrabalho:

- **Escalabilidade:** a capacidade do sistema de ser facilmente ampliado para atender o aumento da utilização, preferencialmente, através da simples adição de módulos de expansão, é um requisito fundamental para a empresa assegurar a manutenção do investimento em equipamentos já instalados.
- **Flexibilidade de Configuração:** É importante que o site central da empresa esteja capacitado a operar com diversos serviços de telecomunicações, tais como linha comutadas, ISDN e *Frame Relay*.
- **Segurança:** A questão da segurança é crítica para a implementação do teletrabalho.
- **Soluções completas:** Para facilitar o gerenciamento e assegurar a interoperabilidade, é importante que os fornecedores de soluções atendam tanto ao escritório domiciliar do teletrabalhador como ao *site* da empresa.

2.2.9 Recursos de Informática

Embora formas simples de teletrabalho sejam tecnicamente possíveis há décadas, somente com desenvolvimento de tecnologias amigáveis o teletrabalho pôde ser viabilizado em larga escala (DUNNING, 1997). Os complexos sistemas do início dos anos 70 foram substituídos, nos anos 80 e 90, por microcomputadores

dotados de interfaces GUI (Graphic User Interface), tais como o Windows Motif e Web (LAUDON, 1999).

O teletrabalho pode ser realizado em um simples terminal de computador. Quase sempre, contudo, um computador de mesa (desktop) ou portátil (notebook), rodando um sistema operacional com interface gráfica Windows ou similar é empregado para a realização das tarefas.

Para facilitar o gerenciamento, Behamou (1998) recomenda a padronização da plataforma e dos aplicativos empregados pelos teletrabalhadores. Além do computador, o teletrabalhador geralmente emprega os mesmos equipamentos disponíveis em um escritório informatizado, tais como: secretária eletrônica, fax, impressora, *scanner*, *webcam*, fotocopiadora, *e-Board* (quadro eletrônico) e programas aplicativos (SCHILL, 1999).

Além de empregar programas aplicativos convencionais, tais como editor de textos, planilhas, bancos de dados, e aplicativos para troca de informações via Internet, como E-mail (SCHILL,1999) dependendo de suas atividades, o teletrabalhador pode empregar programas colaborativos específicos para facilitar o *groupware* (trabalho em grupo) e sistemas baseados na Internet e em Intranets, capazes de formar equipes de trabalhadores dispersos geograficamente (BEHAMOU, 1998; SPARROW, 2000). Tais aplicativos permitem aos usuários compartilhar recursos comuns e facilitam a troca de mensagens, documentos e arquivos. A complexidade dos mesmos, contudo, pode criar dificuldades de manutenção e suporte (VERAS OLIVEIRA, 1996), limitando-os, por vezes, a usuários com muita experiência.

Behamou (1998) recomenda a adoção de padrões da Internet de forma a facilitar a interoperabilidade entre o sistema do teletrabalhador e o da empresa, destacando:

- **Protocolo:** TCP/IP
- **Formato de texto:** HTML e HTTP
- **E-mail:** IMAP4, MIME, POP3 e SMTP
- **Chat e Newsgroup:** IRC e NNTP
- **Troca de dados:** Modelos CORBA e IIOP
- **Sistema de diretórios:** LDAP
- **Protocolos de segurança:** Certificação S/MIME, SSL e X.509

Novos produtos, integrando facilidades operacionais e telecomunicações, tais como soluções de fax, telefonia móvel de terceira geração (tecnologia GSM) com facilidades de telemática móvel, telemetria a tráfego de sistemas, teleconferência, e audioconferência, vem sendo criados de forma a facilitar especificamente o teletrabalho (SIEMENS, 2001).

Por fim, a utilização de canais de alta velocidade, como os disponíveis na Internet II, possibilitam formas avançadas de teletrabalho, como a telepresença médica (manipulação remota de aparelhos biomédicos), permitindo a cirurgiões operarem pacientes situados em regiões remotas, por exemplo, em outros países. (SABBATINI, 1993).

2.2.10 Implantação e Gerenciamento do Teletrabalho

Segundo Steil e Barcia (2000), a literatura sobre a implantação do teletrabalho no domicílio é vasta, configurando-se em sua grande maioria em abordagens prescritivas elaboradas por empresas de consultoria, que abordam as tarefas que são apropriadas ou não para o teletrabalho, tecnologias de suporte e monitoramento, ignorando o fato de que a implantação do teletrabalho demanda uma mudança cultural na organização.

A estratégia de implementação de um programa de teletrabalho varia de empresa para empresa e deve ser feita passo a passo (BEHAMOU, 1998). Nilles (1997) sugere a implantação do teletrabalho na empresa como um projeto piloto para que o mesmo possa ser avaliado com mais segurança pela administração. Para esse autor o teletrabalho deve começar com um pequeno percentual de funcionários da empresa até se avaliarem os impactos, benefícios e, então, possivelmente se aumentar esse número.

Para Trope (1999), a implantação do teletrabalho pode causar um choque cultural ao se trocar o lugar de trabalho conhecido por um ambiente isolado, podendo afetar ainda o sentimento que o teletrabalhador possui de pertencer à empresa. Dziak (apud DUNNING, 1997), atenta para o fato de que muitos programas de teletrabalho falharam por não terem preparado suficientemente os envolvidos no processo para a transição do trabalho convencional para o

teletrabalho. Para esse autor, o teletrabalho só obtém sucesso quando torna-se o resultado de um esforço conjunto dos empregados e empregadores.

Behamou (1998) recomenda a implantação do teletrabalho em 15 passos, por meio dos quais as chances de sucesso do programa serão maximizadas:

1) Elaborar e apresentar a proposta de teletrabalho;
2) Criar um comitê para implementação do teletrabalho;
3) Definir os parâmetros do programa;
4) Desenvolver uma política de teletrabalho para a organização;
5) Desenvolver um contrato de trabalho para teletrabalho;
6) Desenvolver critérios de avaliação do programa;
7) Determinar as necessidades de tecnologia e equipamentos;
8) Desenvolver recursos e material de referência;
9) Implementar o gerenciamento de objetivos;
10) Apresentar orientações para o programa de teletrabalho;
11) Iniciar o programa;
12) Administrar a avaliação do programa;
13) Analisar e preparar os resultados da avaliação;
14) Apresentar os resultados e
15) Efetuar os ajustes necessários.

Behamou (1998) acrescenta que a implantação de um programa de teletrabalho exige o envolvimento de diversas áreas da empresa, tal como a diretoria, jurídica, recursos humanos, treinamento, suporte, telecomunicações, pesquisa e relações públicas.

Segundo Berry (1996), o ponto crucial para o sucesso da implantação de um programa de teletrabalho não é tecnológico, mas sim a compreensão de como ocorre a comunicação entre o teletrabalhador com outros indivíduos na empresa, razão pela qual recomenda uma verificação sobre como ocorre esse processo, para que o mesmo seja simulado através do sistema de teletrabalho.

O treinamento tanto para os teletrabalhadores quanto para os telegerentes e os não-teletrabalhadores que têm contato com esses profissionais é, portanto, de suma importância, indispensável mesmo (STEIL e BARCIA, 2001). Segundo Cascio (2000), o treinamento formal para o teletrabalho pode ser dividido em: treinamento

de teletrabalhadores, treinamento de supervisores e gerentes e treinamento de equipes, nos quais trabalhadores e gerentes poderão aprender e discutir juntos questões que afetam seu relacionamento e aprender com empregados que já tenham experiências pregressas de teletrabalho.

Segundo Nilles (1997), normalmente o treinamento para todos os envolvidos é feito durante a fase de implantação do sistema e, posteriormente, encontros regulares podem ser realizados para manter o espírito de grupo, bem como, para evitar a perda de identidade da equipe.

O gerenciamento do teletrabalho deve ser bem mais cuidadoso do que o do trabalho convencional. Muitos programas de teletrabalho fracassaram por não ter tido planejamento suficiente para a transição (TROPE, 1999).

Os princípios essenciais para o teletrabalho funcionar não são particularmente difíceis ou revolucionários. São simplesmente os bons princípios gerenciais da administração (MELLO, 1999). Nesse sentido, são fundamentais o estabelecimento de diretrizes de trabalho, metas a serem atingidas e uma metodologia de avaliação do desempenho, acordada entre a empresa e os teletrabalhadores.

A administração tradicional se baseia em dois tipos de controle: regras e observação visual do processo de trabalho (KUGELMASS, 1996). A ausência de qualquer supervisão direta constitui uma das maiores diferenças entre o teletrabalhador e o trabalhador tradicional. Na organização virtual o funcionário é cobrado pelo resultado atingido pelo trabalho realizado, e não pela sua presença no ambiente físico da empresa (TROPE, 1999).

Conforme demonstra a figura 2.5, para que um programa de teletrabalho seja bem sucedido, sua implementação e gerenciamento devem ser feitos em passos, e mantidos em contínuo processo de avaliação e ajustes.

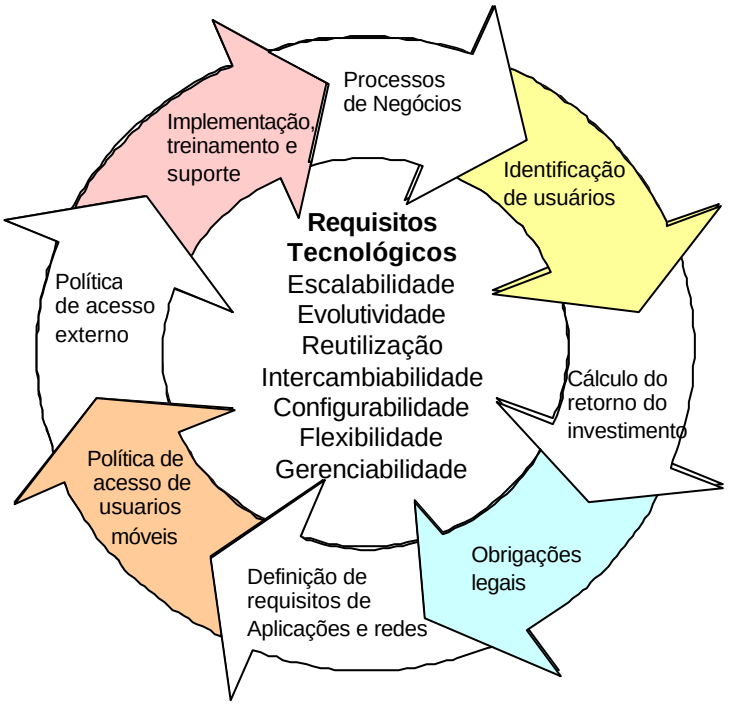

Figura 2.5: Gerenciamento do Teletrabalho com Visão de 360º

Fonte: Gartner Group, 1999.

2.2.11 Custos e Benefícios do Teletrabalho

Nilles (1997) aponta para o fato de que tanto os custos quanto os benefícios do teletrabalho mudam com o tempo. Segundo esse autor, os custos do teletrabalho tendem a aparecer primeiro ao passo que os benefícios se fazem sentir mais lentamente, aumentado mesmo após dois anos de implementado.

Algumas empresas podem oferecer toda a infraestrutura para o teletrabalhador, ao passo que outras se limitam a financiar alguns itens, tais como computadores e móveis (TROPE, 1999). É comum ainda que a empresa não ofereça qualquer facilidade para montagem do escritório do teletrabalhador (NILLES,1997).

Segundo Schill (1999), para empresas de pequeno e médio porte, os custos e os benefícios financeiros são os principais fatores que influenciam na decisão de se implantar o teletrabalho, que variam conforme o cenário, descrito anteriormente no Item 2.9.

Uma das motivações principais para as empresas adotarem o teletrabalho é a melhoria da produtividade e do trabalho realizado. Experiências mostram que o teletrabalhador é mais produtivo do que o trabalhador clássico devido a uma melhor qualidade de vida e uma maior autonomia (TROPE, 1999).

Empresas multinacionais com grande número de funcionários dispersos por dezenas de países vêm empregando teletrabalhadores para reduzir seus custos (WHITFORD, 2000). Esse é o caso da AT&T que tem investido centenas de milhões de dólares em iniciativas de teletrabalho para eliminar escritórios desnecessários e reduzir custos (SPARROW, 2000). Estima-se que, em 2002, o governo americano economizará 750 milhões de dólares por ano através do emprego de teletrabalhadores. Estudos realizados nos Estados Unidos mostram ainda que a redução de custos das empresas quando um funcionário passa a trabalhar em sua residência pode chegar a 30%, com o gasto médio por funcionário caindo de 20 mil para 14 mil dólares anuais (TROPE, 1999).

Segundo o levantamento *1999 TELEWORK AMERICA NATIONAL TELEWORK SURVEY* feito pelo *The International Telework Association and Council*, estima-se que a economia por trabalhador pode chegar a U$ 10.000 anualmente, provenientes da redução do absenteísmo, incremento da produtividade e custos de recrutamento. Além desses fatores, a ETO (2001) também cita como fatores de produtividade a redução dos custos com *turnover* e realocação de pessoal quando se adota o teletrabalho.

O teletrabalho ainda permite um ganho financeiro e competitivo para as empresas quando elas empregam teletrabalhadores localizados em regiões com menor custo de mão de obra (TROPE, 1999), tais como áreas rurais e em comunidades isoladas, como as existentes na Ásia e no Pacífico (DUNING, 1997), podendo ainda contribuir com a revitalização econômica de certas regiões carentes (ETO, 2001).

2.2.12 Vantagens e Desvantagens do Teletrabalho

Como qualquer outra atividade humana, o teletrabalho pode apresentar vantagens e desvantagens para os envolvidos, sejam empregados ou

empregadores, enumeradas por diversos autores (NILES, 1997; DUNNING, 1997; REYMERS, 1998; KUNDU, 1999; KURLAND, 1999; MELLO, 1999; MANN, 2000):

Vantagens potenciais: maior oferta de empregos, maior satisfação com o trabalho, economia de tempo, redução de congestionamentos de tráfego, redução da poluição do ar, melhoria na qualidade de vida, maior disponibilidade de tempo para a família, hobby e lazer, aumento da produtividade, flexibilização do espaço de trabalho, redução do *turnover*, redução do absenteísmo, redução do estresse, redução de custos de transporte, alimentação e vestuário, maior autonomia, agenda flexível, ausência de "política no trabalho", incrementos nas atividades pessoais comunitárias.

Desvantagens potenciais: Isolamento, *overtime*, falta de suporte, prejuízo à carreira, custos com infraestrutura, distração com questões familiares, prejuízo ao espírito de negócios da empresa, falta de espaço físico, problemas legais, problemas com segurança da informação.

Algumas possíveis vantagens arroladas pela teoria do teletrabalho podem vir a ser contestadas na prática, tal como a redução do tráfego nas grandes cidades, que, segundo as evidências, não tem sofrido impacto com a adoção do teletrabalho (REYMERS, 1998). Dada a diversidade dos casos, algumas vantagens do teletrabalho podem ainda, paradoxalmente, constituir-se em desvantagens para empresa ou para o teletrabalhador (ROGNES, 1996)

O teletrabalho, segundo Mello (1999), deveria beneficiar tanto os empregados quanto os empregadores, sendo recomendável, portanto, evitar a adoção do teletrabalho apenas por medida de redução dos custos da empresa.

O teletrabalho pode ser um importante instrumento de justiça social ao possibilitar que deficientes físicos, gestantes, mães e idosos possam exercer atividades profissionais e remuneradas (JAMIL, 2001). Pode também levar oportunidades de trabalho para regiões distantes e economicamente pouco desenvolvidas, tal como algumas regiões da Ásia e do Pacífico que empregam teletrabalhadores para atender grandes centros urbanos da América do Norte (DUNNING, 1997).

Percebe-se que a maior autonomia do teletrabalhador aumenta o *empowerment* ao assumir responsabilidade e o *employeeship*. No primeiro, responsabilidades e poder são delegados pela empresa ao passo que no segundo partem do funcionário. Além disso empowerment e *employeeship* são tendências de descentralização que vão de encontro às necessidades das organizações virtuais ou não (TROPE, 1999).

Com a evolução desse processo, através das redes de comunicação de dados, eliminou-se a noção de pausa para descanso, horários e feriados, instituindo-se a “semana de 168 horas de trabalho” (KUGELMASS, 1996) que, freqüentemente pode significar em uma sobrecarga de atividades para o teletrabalhador.

Para as empresas, o maior benefício do teletrabalho talvez seja o aumento da produtividade. Diversas empresas relataram ganhos de 25 a 60% da produtividade. (REYMERS, 1998). Em uma pesquisa realizada em 1993 pela AT&T junto a gerentes de companhias que possuíam teletrabalhadores, 63% demonstraram um aumento na produtividade (MERIDIAN, 1997). Os motivos desses ganhos de produtividade não são claros, devendo-se provavelmente, em muitos casos, à prática de um número excessivo de horas de trabalho (REYMERS, 1998).

2.2.13 Conclusões sobre o Teletrabalho

Conforme descrito nas seções anteriores, embora existam centros de teleserviços privativos ou comunitários, geralmente o teletrabalho é exercido na residência do trabalhador. O local reservado ao teletrabalho deve ser adequado em termos ergonométricos para a execução das tarefas e dotado de equipamentos semelhantes aos de um escritório automatizado, podendo ser mais incrementado com relação aos recursos de telecomunicações e programas aplicativos, à medida que as atividades sejam mais complexas e a capacitação do trabalhador seja maior. A seleção de empregados com perfil adequado e seu treinamento são muito importantes para o sucesso da implantação do teletrabalho, que por sua vez poderá proporcionar benefícios mútuos, para a empresa e para o empregado, tais como redução de custos, aumento da produtividade e melhoria da qualidade de vida. Diversos autores enumeram as vantagens e desvantagens do teletrabalho, dentre as quais está a segurança das informações, objeto de pesquisa dessa dissertação.

2.3 Segurança da Informação

2.3.1 O que é Informação e Segurança da Informação

Informação é um dado acerca de alguém ou algo; o conhecimento; segundo a teoria da informação, a medida da redução da incerteza (FERREIRA, 1995). A informação é um recurso que, tal como outros importantes recursos organizacionais, tem um valor para a organização e, conseqüentemente, necessita ser protegido. Pode existir de diversas formas: impressa em papel, armazenada eletronicamente, transmitida por correio ou por meios eletrônicos, exibida em filmes ou falada durante uma conversação (ISO/IEC 17799:2000).

Sistema de Informação (SI) é um conjunto de componentes inter-relacionados trabalhando juntos para coletar, recuperar, processar, armazenar e distribuir informação. A finalidade de um sistema de informação é facilitar o planejamento, o controle, a coordenação, a análise e o processo decisório em empresa e em outras organizações (LAUDON, 1999).

Segurança é o ato ou efeito de segurar; estado, qualidade ou condição de seguro; condição daquele ou daquilo em que se pode confiar (FERREIRA, 1995).

Segurança da Informação, por sua vez, conforme definido pela norma ISO 17799, é a proteção contra um grande número de ameaças às informações, de forma a assegurar a continuidade do negócio, minimizando danos comerciais e maximizando o retorno de investimentos e oportunidades.

A segurança da informação é caracterizada pela preservação dos seguintes atributos básicos (ISO/IEC 17799:2000):

a) ***Confidencialidade:*** segurança de que a informação pode ser acessada apenas por quem tem autorização;
b) ***Integridade:*** certeza da precisão e do completismo da informação e
c) ***Disponibilidade:*** garantia de que os usuários autorizados tenham acesso à informação e aos recursos associados, quando necessário.

A preservação desses atributos constitui o paradigma básico da Norma Internacional para Gerenciamento da Segurança da Informação, a ISO 17799, e de toda a ciência da Segurança da Informação.

Segundo Caruso (1999), segurança, mais do que estrutura hierárquica, homens e equipamentos, envolve uma postura gerencial, o que ultrapassa a tradicional abordagem da maioria das empresas.

2.3.2 Normas de Segurança

Um dos maiores obstáculos à implementação da segurança da informação nas empresas é a falta de padrões com relação à metodologia de implementação de soluções (COBB, 2001). Assim, ao longo dos últimos anos, a crescente preocupação com esta questão levou a diversas iniciativas no sentido de se criar critérios de segurança efetivos e suficientemente abrangentes para serem aplicados na maioria das organizações. Foi assim, com este objetivo, que surgiram a Mil-Std-2167A, o Orange Book, o Common Criteria, a BS7799 e a ISO 17799 (BRYDEN, 2001).

As primeiras abordagens da ISO quanto à segurança da informação surgiram com as normas ISO 7948-2 e a IS 15408. A ISO 7748-2 descreve os mecanismos e procedimentos de segurança associados ao modelo de referência OSI (Open Systems Interconnection) empregado no desenvolvimento de sistemas de comunicação em redes. A IS 15408, mais conhecida como *Common Criteria,* foi homologada em 1999 por uma associação de organizações americanas (NIST e NSA) e de outros países (Canadá, França, Alemanha, Holanda e Inglaterra) com o objetivo de identificar e avaliar facilidades de segurança para computadores e sistemas, e subsidiar os desenvolvedores desses sistemas (SANTILLO, 2001). A dificuldade da implementação do *Common Criteria,* contudo, tem levado a indústria a ignorá-lo (BRYDEN, 2001).

A BS7799, por sua vez, foi criada com objetivo de promover o planejamento da segurança no mundo comercial (ROBIETTE, 2001) e subsidiar empresas na elaboração de suas políticas de segurança.

A ISO 17799 é a versão internacional da BS7799. O esforço do qual resultou a norma remonta à 1987, quando o departamento de comércio e indústria do Reino Unido (DTI) criou um centro de segurança de informações, o CCSC (Commercial

Computer Security Centre), que, dentre suas atribuições, tinha a tarefa de criar um código de segurança para os usuários das informações, por meio da criação de critérios para avaliação da segurança (SOLMS, 1998). Com base nesse objetivo, em 1990 foi publicada a primeira versão do código de segurança, denominado PD0003 – *Code to Information Security Management*, que, em 1995, foi revisado e publicado como um *Britsh Standart*, a BS7799:1995. Em 1996, essa norma foi proposta ao ISO para homologação mas foi rejeitada (HEFFERAN, 2000).

Uma segunda parte desse documento foi criada posteriormente e publicada em novembro de 1997 para consulta pública e avaliação. Em 1998 esse documento foi publicado como BS7799-2:1998 e, após uma significativa revisão (COBB, 2001), foi publicado em abril de 1999 como BS7799:1999 (HEFFERAN, 2000).

Ao longo de seu desenvolvimento, a norma BS foi sendo adotada não só pela Inglaterra como também por outros países da Comunidade Britânica, tal como Austrália, África do Sul e Nova Zelândia (SOLMS, 1998).

Através de uma associação entre o Information Technology Committee da ISO e da International Electro-technical Commission (IEC), em 2000 a norma foi aprovada em regime de *fast-track* (STACEY, 2000), sendo homologada como ISO/IEC 17799:2000 em dezembro de 2000 (MÓDULO, 2001). Com a homologação da norma ISO, a ABNT (Associação Brasileira de Normas Técnicas) criou, em 2001, a norma brasileira de segurança da informação, denominada NBR ISO/IEC 17799.

Com o surgimento da norma ISO e da norma brasileira, também serão criados os processos de *Certificação de Segurança* baseados nessas normas, que empresas e organizações poderão obter ao aplicar os controles previstos nas normas, demonstrando para o mercado a importância dada pela empresa à segurança de suas informações.

Cobb (2001) atenta para o fato que a BS7799 e, conseqüentemente, a ISO 17799, são muito direcionadas à implementação da segurança da informação na área de negócios, o que pode implicar em maiores dificuldades ao se tentar implementá-las em outros tipos de organizações. Robiette (2001) afirma o mesmo, frisando ser difícil implementar a BS7799 em uma universidade. Bryden (2001) por sua vez, discorrendo sobre os problemas da implementação dos padrões nas empresas, alerta para o risco de se tomar as normas como panacéia para todos os problemas de segurança da informação, acreditando-se que a norma, por si só, garantirá a segurança. Esse autor também considera o desconhecimento dos

padrões como um problema básico para sua implementação, mas sugere que é preferível ter padrões de segurança do que não tê-los.

A figura 2.6, baseada em um modelo de Fagan (2000), com modificações, mostra os componentes da norma ISO e seus relacionamentos, descritos a seguir:

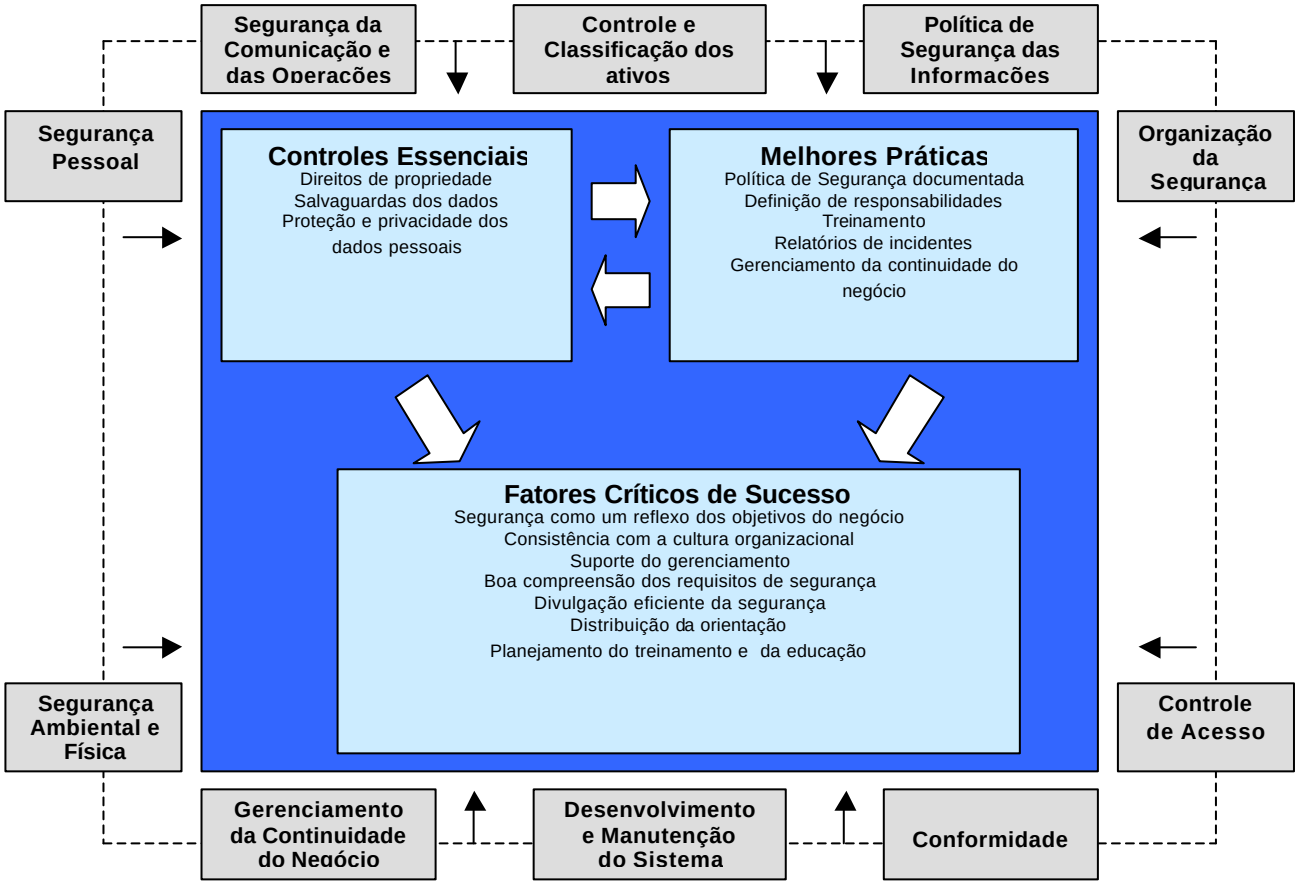

Figura 2.6: Componentes da ISO 17799

Fonte: Adaptado de Fagan, 2000.

(A) Organização da Segurança: Uma estrutura de gerenciamento deve ser estabelecida para iniciar e controlar a implementação da segurança da informação na empresa;

(B) Controle de acesso: O acesso à informação deve ser controlado com base nos requisitos de segurança estabelecidos pela organização;

(C) Conformidade: Deve-se evitar a violação de leis, estatutos, regulamentações ou obrigações contratuais e de quaisquer requisitos de segurança.

(D) Desenvolvimento e manutenção do sistema: Deve-se garantir que a segurança está implantada nos sistemas de informação da empresa;
(E) Gestão da continuidade do negócio: Não deve ser permitida a interrupção das atividades da organização, e deve-se proteger os processos críticos contra os efeitos de falhas e desastres;
(F) Segurança ambiental e física: Devem ser tomadas medidas preventivas para prevenir o acesso não autorizado , dano e interferência nas instalações físicas das organização e à sua informação;
(G) Segurança pessoal: Devem ser tomadas medidas de segurança quanto ao recrutamento e gestão dos recursos humanos, incluindo cláusulas contratuais quanto ao acesso a informações sensíveis;
(H) Gerenciamento da comunicação e das operações: Deve ser mantida a integridade e a disponibilidade dos serviços de comunicação e processamento da informação;
(I) Controle e classificação dos ativos: Todos os principais ativos de informação da organização devem ser inventariados e devem ter um proprietário responsável e
(J) Política de segurança das informações: A política deve ser aprovada pela administração da empresa e comunicada de forma adequada para todos os funcionários.

A ISO 17799 é uma metodologia *top-down* abrangente, baseada em controles de gerenciamento (ROBIETTE, 2001) que objetiva contemplar todos os aspectos da segurança da informação e proporcionar segurança organizacional para produtos, prestação de serviços e de parcerias comerciais (COBB, 2001). A norma brasileira segue a mesma estrutura de capítulos, itens e controles da ISO 17799.

Como a ISO 17799 cobre os mais diversos tópicos da área de segurança, possuindo mais de 100 controles que devem ser atendidos para garantir a segurança das informações de uma empresa, a obtenção da certificação pode ser um processo demorado e muito trabalhoso, consistindo num desafio para as empresas.

2.3.3 Projeto de Segurança

A estratégia de segurança da informação de uma empresa exige a elaboração de um *projeto de segurança* que descreve todos os aspectos da segurança da informação para esta empresa. Um desses aspectos consiste na elaboração de um *plano de segurança*, ou seja, um documento de alto nível onde são elencadas as medidas que serão tomadas pela organização para satisfazer a requisitos de segurança considerados necessários, contendo a relação dos serviços de TI disponibilizados, quais áreas da empresa disponibilizam os serviços, quem terá acesso aos serviços, a descrição detalhada de sua implementação, dos procedimentos de controle dos ambientes, incidentes e contingências (FRASER, 1997; OPPENHEIMER, 1999). O projeto de segurança, segundo Oppenheimer (1999), envolve várias etapas de trabalho:

(1) Identificação dos ativos da empresa em termos de informações;
(2) Análise dos riscos de segurança;
(3) Análise dos requisitos de segurança e compromissos;
(4) Desenvolvimento de um plano de segurança;
(5) Definição de uma norma de segurança;
(6) Desenvolvimento de procedimentos para implantar a norma e uma estratégia de implementação e
(7) Implementação, gerenciamento e auditoria dos procedimentos de segurança.

Segundo Fraser (1997), a *norma de segurança* é uma declaração formal de regras através das quais as pessoas têm um determinado acesso à tecnologia e aos ativos de informações de uma organização. A norma de segurança informa quais são as obrigações dos gerentes e do pessoal técnico e especifica quais mecanismos devem ser empregados para cumprir com essas obrigações (OPPENHEIMER, 1999).

Com base na norma de segurança, é criado um documento denominado *política de segurança* para ser divulgado em toda empresa. Para implementar a política de segurança deve ser criada um *arquitetura de segurança* que consiste na aplicação de todos os controles físicos, lógicos, técnicos e administrativos

necessários para assegurar a informação (ROBERTI, 2001). Com base nessa arquitetura, são criados, ainda um plano de contingência e um processo de auditoria.

O conjunto de todos os controles, procedimentos e mecanismos de segurança, conforme apresentado na figura 2.7, denomina-se *modelo de segurança*. Se esse modelo for corretamente implementado, pode reduzir o custo do desenvolvimento e do gerenciamento da segurança (BENSON, 2001).

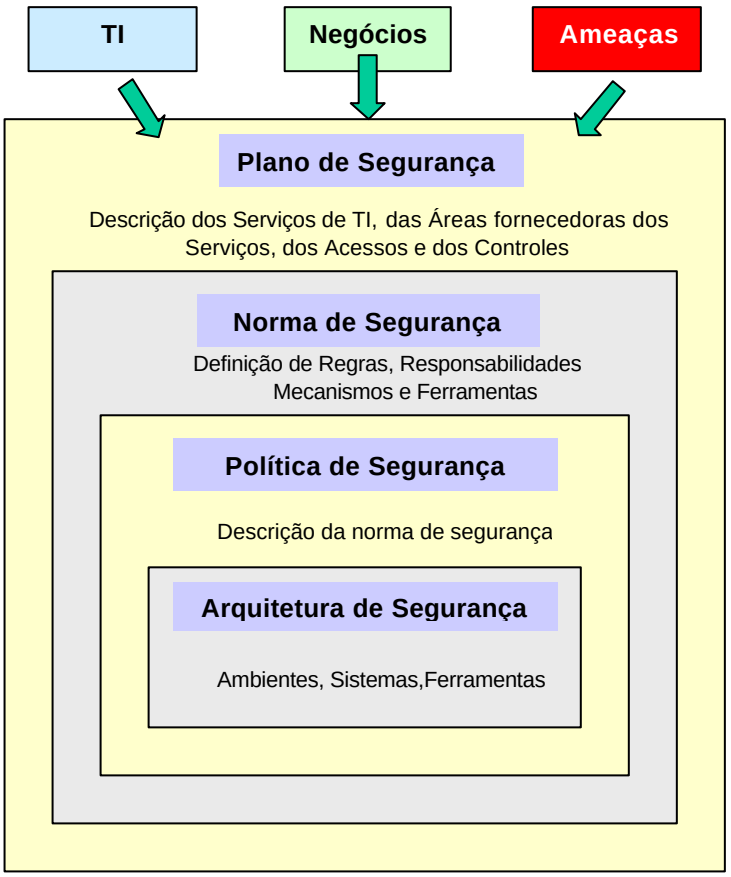

Figura 2.7: Componentes de um Modelo de Segurança

2.3.4 Análise de Riscos

Os requisitos de segurança necessários para uma organização são identificados através de uma análise metodológica dos riscos de segurança. A análise de riscos pode ser aplicada a toda organização ou a uma parte da mesma, ou ainda a um determinado sistema de informações, necessitando, para tanto, que sejam classificadas as informações da empresa de forma a indicar seu grau de

importância, a prioridade e o nível de proteção necessário (ISO/IEC 17799:2000). Gutterman (1997) sugere a classificação das informações em: sensíveis, confidenciais, privativas e públicas.

Segundo Caruso (1999), a análise de riscos envolve aspectos subjetivos em graus variados, conforme o conhecimento que se tem sobre o sistema a ser avaliado e o sistema de avaliação, o que significa que não se pode esperar por uma análise perfeita mas sim pela melhor possível. Ainda, segundo Caruso (1999), a análise de riscos geralmente pode ser feita calculando-se o valor econômico das informações a serem protegidas e o grau de risco para essas informações, que a grosso modo poderia ser: baixo, médio e médio.

Os riscos podem variar desde intrusos hostis a usuários que transferem aplicativos da Internet contendo vírus. Os intrusos podem roubar, adulterar ou destruir os dados do usuário ou podem fazer ataques do tipo negação de serviço (OPPENHEIMER, 1999).

Segundo o *2001 CSI/FBI Computer Crime and Security Survey,* as principais ameaças à segurança da informação no ano de 2001 são:

- **1º Lugar:** Vírus de computador
- **2º Lugar:** Uso interno indevido do acesso a rede
- **3º Lugar:** Roubos de *notebooks*
- **4º Lugar:** Acesso interno não autorizado
- **5º Lugar:** Penetração externa no sistema

Outras ameaças descritas nesse relatório incluem sabotagem, fraudes e escuta telefônica. O relatório observa ainda que é crescente o número de ameaças oriundas da Internet e que a principal causa de perdas financeiras são os vírus de computador.

Segundo Fraser (1997), o paradigma básico com relação à segurança é que os recursos empregados para assegurar a informação devem ter um custo menor do que o de recuperar a informação se uma ameaça o atingir, sendo o custo expresso em moeda corrente, reputação, confiabilidade ou outras medidas menos óbvias.

A figura 2.8 é baseada num modelo de Fagan (2000) e demonstra como é formulada a análise de risco.

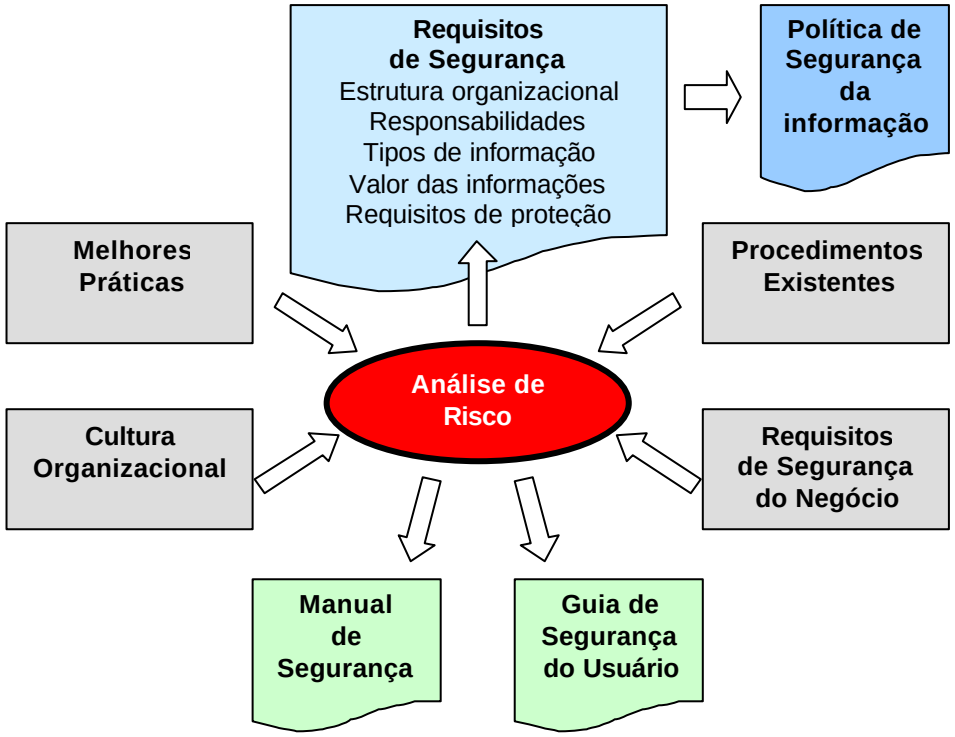

Figura 2.8: Formulação da Análise de Risco

Fonte: Fagan, 2000.

2.3.5 Política de Segurança

Por política de segurança entende-se a política elaborada, implantada e em contínuo processo de revisão, válida para toda a organização com regras mais claras e simples possível e estrutura gerencial e material de suporte a essa política, claramente sustentada pela alta hierarquia da empresa (CARUSO, 1999).

Fraser (1997) define política de segurança como um conjunto de regras formais, às quais as pessoas, a quem for dado acesso os sistemas tecnológicos e informacionais da empresa, devem obedecer.

Segundo a ISO/IEC 17799:2000, a política de segurança tem por objetivo prover a administração de uma direção e apoio para a segurança da informação. Segundo Fraser (1997), o principal propósito da política de segurança é informar aos usuários, a equipe e os gerentes quais são os requerimentos obrigatórios para proteger o sistema de informação da empresa. A política pode especificar os mecanismos através dos quais esses requerimentos serão atendidos e proporcionar a base para obter, configurar e auditar sistemas computacionais e redes em conformidade com essa política. Segundo Fraser (1997), as características de uma boa política de segurança são:

(1) Deve ser implementada através de sistemas administrativos, publicada na forma de norma ou divulgada por algum outro método apropriado;
(2) Deve ser implementada através de ferramentas de segurança onde for possível e prever sanções quando não for tecnicamente possível a prevenção e
(3) Deve definir claramente as responsabilidades de usuários, administradores e gerentes.

A ISO 17799 acrescenta ainda os seguintes princípios a serem seguidos pela política de segurança:

(1) Conformidade com a legislação e cláusulas contratuais;
(2) Requisitos na educação de segurança;
(3) Prevenção e detecção de vírus e *softwares* maliciosos;
(4) Gestão e continuidade dos negócios e
(5) Conseqüências das violações na política de segurança.

A figura 2.9 demostra os componentes da política de segurança e seus relacionamentos.

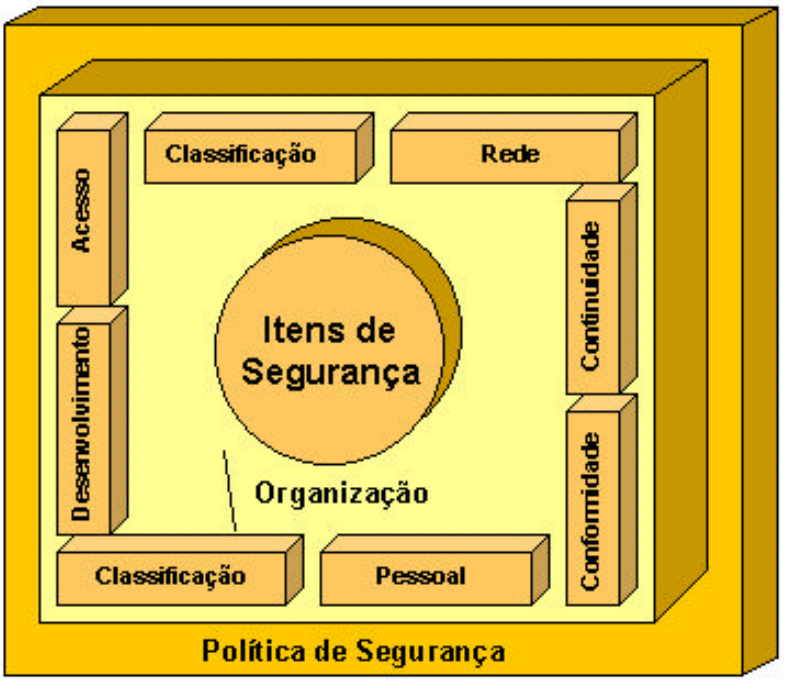

Figura 2.9: Componentes da Política de Segurança

Fonte: Coutanche, 2001

Uma vez aprovada, a política de segurança deve ser publicada e divulgada para todos os funcionários da organização (ISO/IEC 17799:2000). Seu conteúdo mínimo deve conter objetivos, aplicabilidade, responsabilidades, análise de riscos, segurança física, segurança lógica, conformidade e generalidades (GUTTMAN, 1997; CARUSO, 1999).

Por fim, a política de segurança deve ser genérica o suficiente para que não venha a sofrer grandes alterações muito rapidamente, procurando para tanto ser independente, na medida do possível, do *hardware* e do *software* em uso no sistema (FRASER, 1997).

2.3.6 Plano de Contingência e Auditoria

O plano de contingência deve ser criado para as empresas altamente dependentes dos sistemas de informações, consistindo na elaboração de um conjunto de medidas para recuperação de falhas e de desastres, tais como incêndios, inundações, interrupções de energia e sabotagens (LAUDON, 1999).

O plano de contingência consiste na criação de backups dos dados, identificação dos pontos mais vulneráveis do sistema, a criação de redundâncias para os mesmos e treinamento do pessoal para seguir o plano corretamente (LAUDON, 1999).

Para analisar a segurança da rede e responder a incidentes de segurança, procedimentos de auditoria devem ser estabelecidos para coleta de dados de atividades da rede. Esta coleta é denominada *auditoria* (OPENHEIMER, 1999).

A auditoria quanto à segurança da informação no sistema de TI envolve a auditoria dos aspectos físicos, lógicos e pessoais relacionados ao sistemas, podendo ser realizada de forma geral, parcial ou por amostragem (MAGALHÃES, 2001).

Em 1999 a ISACF (Information Systems Audit and Control Foundation) homologou uma metodologia de auditoria para sistemas de TI denominada COBIT (Control Objectives for Information and Related Technology) (LAINHART, 2001), sendo esta a mais completa metodologia aplicável a verificação da segurança da informação nas organizações da atualidade.

A COBIT é uma metodologia de auditoria genérica, criada para atender a atual necessidade das organizações que possuem complexos sistemas de informações. A COBIT divide as atividades de TI em 5 domínios (recursos de TI, planejamento/organização, aquisição/implementação, entrega/suporte e monitoração), 34 controles e 302 pontos passíveis de serem auditados (LAINHART, 2001). O objetivo da metodologia é, através desses controles, não impactar o fluxo das atividades e trocas de informações na organização, mas pelo contrário, viabilizá-lo (LAINHART, 2001).

2.3.7 Ferramentas de Segurança

Ao longo do processo de evolução da segurança da informação, diversas ferramentas foram criadas com a finalidade de proteger o acesso às redes e sistemas de informações das empresas.

Dentre as inúmeras ferramentas de segurança atualmente disponíveis, assim como suas respectivas variações, são relacionadas a seguir as principais ferramentas no mercado para implementação da segurança da informação, e citadas

nos próximos capítulos dessa pesquisa, cujas características e funcionamento são detalhadamente descritas por diversos autores (FRASER, 1997; OPPENHEIMER, 1999; TEIXEIRA JUNIOR, 1999; GONÇALVES, 2000; SCHNEIER, 2001):

- Antivírus: *Software* capaz de detectar e eliminar viroses de computador, assegurando a integridade e disponibilidade das informações;
- *Backup*: Sistema que possibilita a reprodução e a posterior restauração de informações a partir de meios magnéticos, óticos ou outros;
- Biometria: Sistema de que emprega características biométricas, tal como impressão digital e mapeamento da íris para identificar o usuário;
- *Call-Back*: Sistema onde o usuário remoto somente pode acessar a rede da empresa após o retorno da sua ligação telefônica efetuada pelo servidor de acesso remoto da empresa;
- Criptografia: Processo de codificação e decodificação de dados empregando algoritmos criptográficos matemáticos complexos, protegendo a confidencialidade da informação;
- *Firewall*: Sistema baseado em *software* ou *hardware* capaz de controlar o acesso entre duas redes ou sistemas, impedindo acessos indevidos e ataques;
- IDS: *Intrusion Detection System*. Sistema capaz de identificar a atividade de um invasor na rede e iniciar procedimentos de alerta e contra-ataque;
- PKI : *Public Key Infrastructure*. Processo de certificação digital que possibilita a identificação inequívoca da identidade, procedência e conteúdo das informações, baseado na troca de chaves criptografadas;
- Servidor de Comunicação RADIUS ou TACACS: Sistema de comunicação capaz de concentrar e autenticar, de forma segura, conexões remotas, geralmente por via telefônica, dos usuários do sistema;
- *Token Card*: Sistema de identificação baseado em um cartão de identificação que possibilita a autenticação da identidade do usuário;
- VPN: *Virtual Private Network*. Sistema implementado por *software* ou *hardware* capaz de assegurar uma conexão de dados segura em meios públicos (como a Internet) através de mecanismos de tunelamento, autenticação e criptografia.

O emprego de algumas ferramentas como *firewalls* e anti-vírus é obrigatório face às constantes ameaças. A utilização de outras ferramentas contudo, depende

de uma cuidadosa avaliação dos riscos para a informação e dos custos dos produtos e de sua operação (CARUSO, 1999).

2.3.8 Gerência da Segurança

Para ser efetiva, a gerência da segurança deve se valer de mecanismos, procedimentos e ferramentas adequadas à execução do plano de segurança. Envolve ainda a criação e o treinamento (indispensável) de uma equipe de segurança cuja responsabilidade é implantar e manter o plano de segurança (GOSLAR, 2000), atuando como ponto focal do gerenciamento da segurança (GAO, 1998).

A gerência da segurança deve basear-se na premissa de que não existe política de segurança certa ou errada, ou pronta para uso. Uma vez que é impossível obter-se segurança absoluta, é importante cercar o ambiente de informações com medidas que garantam sua segurança efetiva a um custo aceitável (CARUSO, 1999)

Um sistema de fácil utilização pode ficar mais complexo devido à implementação de certos recursos de segurança da informação, como por exemplo, uma política de senhas fortes (FRASER, 1997).

É importante se estabelecer metas a serem atingidas e uma metodologia de avaliação do desempenho da segurança, mas, segundo Kwok (1999), a segurança da informação é uma variável difícil de ser medida o que pode impossibilitar a criação de índices do desempenho da segurança pouco convincentes. Kwok (1999) alerta ainda para a importância de se ter uma boa documentação de segurança de forma a facilitar análises e estudos.

Caruso (1999) enumera diversos problemas advindos da falta de cultura na empresa quanto a segurança, tal como acreditar que, uma vez implantada a segurança, as informações estão seguras ou que a segurança das informações é de exclusiva responsabilidade da área de segurança.

A área de segurança (security office) normalmente se localiza junto à alta administração de um dado ambiente de informações, de forma a tornar-se menos suscetível a pressões e comprometimentos, tendo ainda o poder de impor procedimentos de segurança (CARUSO, 1999).

Norton (2000) descreve três fases contínuas e contíguas que formam um ciclo de segurança, em constante processo de evolução, com relação ao gerenciamento da segurança na empresa:

(1) Fase de Proteção: implementação e manutenção de medidas de segurança;
(2) Fase de Detecção: detecção, monitoramento e auditoria de incidentes e
(3) Fase de Resposta: ativação de contramedidas, investigação, recuperação de desastres e atualização/adequação da segurança.

Goslar (2000), referindo-se aos fatores que comprometem a segurança da informação arrolados no congresso de profissionais de segurança *SANS'99*, cita como os principais erros de gerenciamento: ignorar os problemas na esperança que desapareçam; adotar medidas reativas acarretando em rápido reaparecimento dos problemas; ignorar o valor das informações e a reputação da empresa; implementar *firewalls* como a única medida de defesa; implementar a segurança com base em procedimentos rápidos do tipo "receita de bolo"; ignorar as relações entre segurança da informação e segurança física e empregar uma equipe sem treinamento para manter a segurança da informação na empresa.

Em um sentido mais amplo, o processo da segurança da informação deve estar em constante evolução e avaliação na empresa, tendo por foco a equipe responsável pela segurança da informação na organização, tal como sintetiza a figura 2.10.

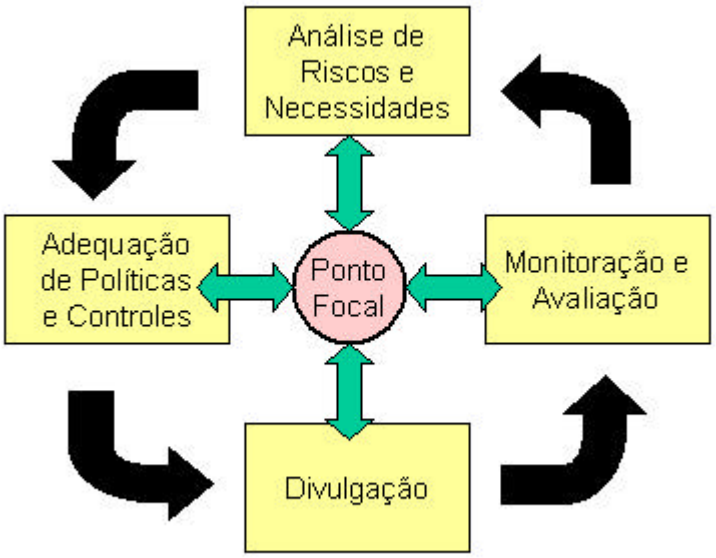

Figura 2.10: Dinâmica do Gerenciamento da Segurança

Fonte: Adaptado do GAO, 1998.

2.3.9 Teletrabalho e Segurança da Informação

O teletrabalho, como parte das atividades negociais, se inter-relaciona com as atividades do sistema de informações das empresas, interagindo em diversos níveis de acesso, seja alimentando-o com novas informações, seja acessando as informações armazenadas.

Contudo, a mesma porta que permite o acesso do teletrabalhador, tal como uma linha telefônica comutada, também possibilita o acesso de intrusos (VERAS OLIVEIRA, 1999) que, ao terem acesso à rede ou sistema de informações da empresa, podem produzir danos variados.

À medida que os meios de comunicação de dados e o acesso a ferramentas tecnológicas vão se popularizando, os riscos vão, proporcionalmente, aumentando para os sistemas de teletrabalho. Tal ocorre, por exemplo, com a popularização das conexões DSL que possibilitam uma conexão permanente do usuário com a Internet, facilitando seu trabalho, mas gerando novos perigos como ataques

baseados em varreduras de portas realizadas por invasores (CHEN, 2000; McADAMS, 1999).

A maioria dos autores, tal como os citados anteriormente (KUGELMASS, 1996; VERAS OLIVEIRA, 1996; TROPE, 1999; MELLO, 1999) admitem a necessidade de cuidados com a segurança da informação em sistemas de teletrabalho, sendo contudo, muito superficiais em suas abordagens. Leonhard (1996), por exemplo, prescreve o uso de ferramentas de segurança pelo teletrabalhador, tais como criptografia, autenticação forte, controle de acesso, VPN , *Token Card*, *dial-backup* e *Firewall*, mas recomenda a leitura de outras obras sobre segurança em microcomputadores PC para obtenção de maiores esclarecimentos.

Ao contrário dos computadores localizados nas instalações da empresa, os postos de trabalho dos teletrabalhadores geralmente recebem pouco ou nenhum acompanhamento por parte dos empregadores, tanto no que se refere a questões de *hardware* e *software* quanto com relação a segurança das informações (VERAS OLIVEIRA, 1996; CHEN, 2000; GOSLAR, 2000).

Nilles (1997) reconhece a gravidade da questão da segurança da informação para o teletrabalho. Citando dados da *Pcweek*, Nilles (1997) alerta para o fato que 8% dos *notebooks* acabam sendo roubados, seja por ladrões comuns, seja por competidores ávidos pelas informações que eles possam conter. Segundo Reid (2000), uma pesquisa realizada pelos fabricantes de *notebooks* em 1999, constatou que nesse ano 319 mil *notebooks* foram roubados em todo mundo. Apesar disso, Nilles acredita que a restrição de acesso do teletrabalhador à informações não críticas restringiria muito seu trabalho, prescrevendo algumas medidas preventivas quanto a segurança das informações: não interligar os mainframes diretamente aos servidores de comunicação; utilização de *token-cards* (cartão com memória eletrônica) com senhas; C*allback*; biometria; criptografia; cuidados como mídias removíveis; cuidados sobre quem vai fazer a manutenção do sistema do teletrabalhador. Ainda, segundo Nilles, deve ser considerado que o teletrabalhador não mora sozinho e que o computador do seu posto de trabalho freqüentemente é compartilhado pela família, sendo responsabilidade do teletrabalhador manter esse posto em condições perfeitamente aceitáveis pela empresa. Segundo o referido autor, inspeções realizadas pela empresa devem ser realizadas nas instalações do teletrabalhador para garantir essas condições, cabendo ainda a esse, informar imediatamente ao supervisor a ocorrência de incidentes ou irregularidades.

Algumas companhias desestimulam o teletrabalho em virtude das preocupações com a segurança (KUGELMASS, 1996; STURGEON, 1996). Por outro lado, Anderson (2000) citando Gil Gordon, afirma que, se em muitas companhias os empregados podem sair levando consigo relatórios, disquetes e outras mídias contendo informações importantes, é incorreto afirmar que a existência de teletrabalhadores representa uma forma de risco maior ou diferente. Certamente, a maior parte das ameaças contra a segurança deriva dos descuidos de certos itens de segurança ou violações feitas por empregados (KUGELMASS, 1996; CSI, 2001).

Por fim, segundo Sturgeon (1996) apesar de algumas empresas ainda proibirem o trabalho com informações sensíveis fora do escritório, a maioria das empresas vêm permitindo que essas atividades sejam realizadas por teletrabalhadores. Ao nível governamental, Sturgeon afirma ainda que essa possibilidade tem sido restringida a gerentes e executivos seniores.

Dentre os diversos problemas relativos à segurança da informação, Dalal (1999), Leonhard (1996), Weissenflus (2000), Girard (1999) e Hirsch (2000), relacionam:

- Conexões por telefone podem ser grampeadas;
- Hackers e empregados desonestos e criminosos *high-tech* podem sutilmente manipular ou destruir dados sensíveis;
- Transferências de arquivos via Internet podem ser monitoradas;
- Viroses e código malicioso que podem contaminar o sistema;
- As informações podem ser roubadas quando o computador do teletrabalhador sofrer suporte e manutenção;
- Pessoas podem ver o teletrabalhador usando *notebook* em lugares públicos digitando sua senha de acesso;
- O sistema operacional normalmente empregado pelos usuários é o Windows 9x que não oferece segurança;
- No lar do teletrabalhador o equipamento está sujeito a riscos e avarias que não existem na empresa, como crianças ou espiões;
- A utilização do computador do teletrabalhador pela sua família pode causar avaria no sistema ou nos dados na medida que instalem certos programas aplicativos;
- Amigos ou a família podem ter acesso ao computador e avariar seus dados;

- Empregados desonestos podem ceder suas senhas para atacantes;
- Hotéis que fornecem serviços de rede podem ter *sniffers* (programas para captura de senhas) instalados;

Com relação às ferramentas e medidas de segurança capazes de reduzir os riscos, Nilles (1997), Chen (2000), Hirsch (2000), Percell (2000), Reid (2000) e Cartwright (2001) recomendam:

- Antivírus nos micros dos usuários;
- *Firewalls* pessoais capazes de deter programas intrusos (trojans);
- Criptografia baseada no aplicativo PGP (Pretty Good Privacy) para arquivos do micro e correio eletrônico;
- *Passphrase* (uma longa senha formada por várias palavras) para acesso ao sistema e aplicações;
- Especial cuidado com mídia removível (Zip Drive, HD, CD-ROM) que devem ter os dados encriptados;
- Emprego de VPN (Virtual Private Network);
- Emprego de *CallBack*;
- Uso de senhas na *Bios*;
- *Backup* do disco rígido;
- Biometria;
- Controle de acesso com uso de permissões limitadas para acesso remoto;
- Vários esquemas de proteção do HD com senhas;
- Encriptação do disco rígido;
- Emprego de *token-cards* com senhas para identificação dos usuários;
- Emprego de *notebooks* cedidos pela empresa, especialmente configurados pela empresa como mecanismos de segurança;
- Emprego de NCs (Network Computers – Computadores para Redes);
- Emprego de *softwares* de acesso remoto seguros;
- Emprego de servidor de comunicação com autenticação RADIUS ou TACACS e
- Auditoria.

Algumas das soluções propostas, tal como o emprego de *Network Computers*, um produto de fornecimento escasso, podem ser incompatíveis com a

realidade técnica e econômica da empresa. Segundo Chen (2000) a maioria dos gerentes de TI concorda que a combinação de VPN e *Call-back* é, geralmente, suficiente para garantir a segurança das informações para um sistema de acesso remoto.

Várias empresas, como a Cisco Systems (2001), fornecem soluções proprietárias para garantir a segurança da informação para teletrabalhadores. Essas soluções contudo, baseiam-se apenas na instalação dos produtos dessas empresas, que, por não fornecerem uma solução completa, recomendam a utilização de checklists de segurança, tal como o disponibilizado pela Smart Valey (2001).

Um outro problema é apontado por Dalal (1999), segundo o qual, como a configuração de perfis de segurança não é tarefa simples, tanto usuários como administradores tendem a tomar o caminho mais curto quanto a configuração, esquivando-se de tomar todas as medidas necessárias, tornando o sistema vulnerável. A figura 2.11 sintetiza as ameaças às quais o teletrabalhador está sujeito.

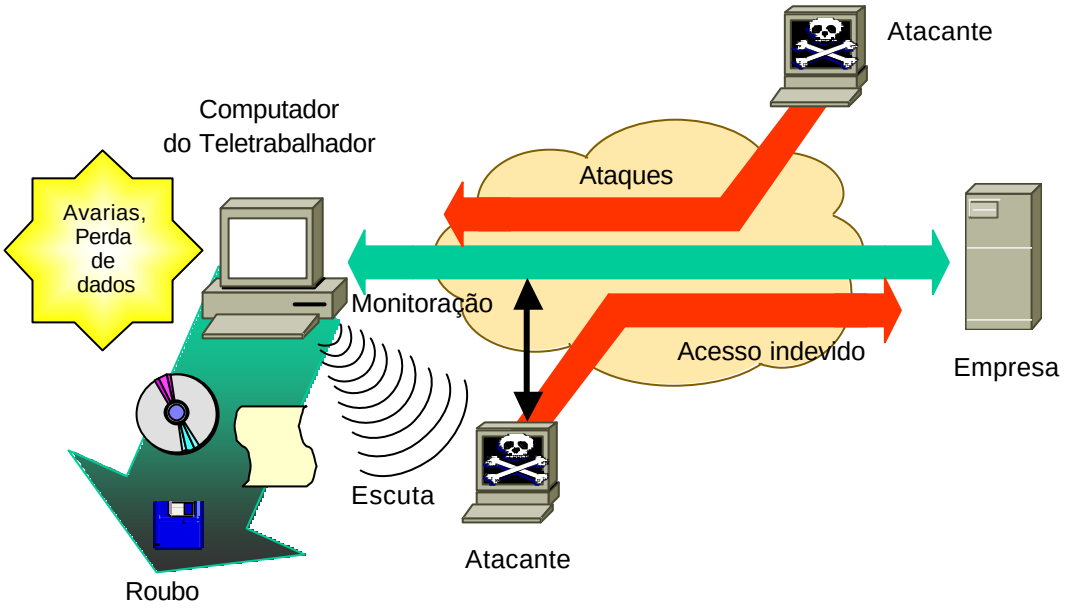

Figura 2.11: Ameaças ao teletrabalhador

Segundo Chen (2000), as empresas geralmente focalizam a segurança da informação sob o ponto de vista de equipamentos e sistemas e não dos empregados, descuidando-se da questão de, por exemplo, fazer um cuidadoso programa de seleção de teletrabalhadores.

Chen (2000) e Goslar (2000) consideram o treinamento dos teletrabalhadores como o fator mais importante para o processo da segurança da informação. Chen cita dados da Pesquisa do FBI de 1999, segundo a qual as perdas com teletrabalho relativas a problemas de segurança da informação nos Estados Unidos chegaram a 66,7 milhões de dólares.

Como menciona Sturgeon (1996), um dos maiores desafios da organização com relação ao teletrabalho é o ajuste cultural necessário, onde um modelo baseado no monitoramento e no controle tem de ceder lugar a um modelo baseado na confiança. Tal situação se manifesta também com relação à segurança da informação, pois, enquanto as informações e os usuários podem ser controlados e monitorados na empresa, o mesmo não é possível no ambiente do teletrabalhador. Esse é um dos motivos pelos quais freqüentemente são adicionadas cláusulas contratuais referentes à segurança da informação para os empregados que desejam teletrabalhar.

Contratos para contratação de teletrabalhadores, tal como o da Deutsch Telekom (TELMET, 2001), prevêem cobertura para segurança de dados e equipamentos e determinam que o empregado deverá ser apropriadamente informado sobre as normas de segurança e proteção de dados. Segundo Chen (2000), conforme medidas de segurança são aplicadas, tal como a padronização de uma nova ferramenta de segurança, os teletrabalhadores devem assinar um documento comprometendo-se a efetuar sua instalação. Com relação a questões contratuais, Chen (2000) também cita os procedimentos do programa de teletrabalho promovido pelo estado do Arizona (EUA), segundo o qual, antes de se tornarem teletrabalhadores, os candidatos devem assinar um contrato onde afirmam ter lido e entendido a política de segurança da informação da empresa. Goslar (2000) considera esses contratos, a serem assinados não só por teletralhadores como pelos executivos responsáveis pela empresa, como essenciais para garantir a segurança das informações.

Como medidas para melhorar a segurança, Chen (2000) e Goslar (2000) recomendam a realização de pesquisas através de questionários preenchidos pelos teletrabalhadores quanto a incidentes e medidas de segurança para atualizar a política de segurança da empresa.

Hirsch (2000) recomenda, como medidas de segurança, a definição de uma política de segurança da informação clara e objetiva para teletrabalhadores

constantemente revisada, que deve abordar pelo menos os seguintes tópicos: equipamentos (hardware e software); orientações para segurança física; medidas para proteção da integridade dos dados (backup, VPN, etc); restrições de *login* e de acesso para o empregado; definição de quais informações não poderão ser acessadas remotamente; plano de recuperação de falhas e desastres; orientações para suporte e manutenção; comprometimento do empregado quanto a integridade e confidencialidade dos dados e orientações apropriadas para o teletrabalhador quanto a segurança da informação.

Para elaborar uma política de segurança para teletrabalhadores, ou ainda, para obter maiores detalhes sobre segurança da informação para teletrabalhadores, podem ser empregados as RFC 2504 (1999) – *Security User Guide* e a RFC 2106 (1997) – *Site Security Handbook*, que são documentos públicos criados pelo IETF, disponíveis na Internet. Contudo, segundo Chen (2000), uma das preocupações dos gerentes está em não confundir os usuários com tantas medidas de segurança. De fato, documentos como as RFCs acima citadas são documentos criados para *experts* na área de informática. Para esse autor, o sucesso de um programa de teletrabalho é um correto balanceamento entre educação, tecnologia e políticas.

Poucas organizações que promovem programas de teletrabalho produzem documentação pública mais detalhada sobre segurança da informação, tal como *Telecommuting Security Guide* do *US Department of Energy - Office of Information Management* (1997). Nesse pequeno guia são relacionados riscos, medidas de segurança, como as já citadas nesse capítulo, e exemplos de contratos com adendos sobre segurança da informação para contratação de teletrabalhadores.

Por fim, a norma ISO/DIS 17799, publicada em 2000, traz no capítulo 9, item 9.8.2, um conjunto de controles que podem ser empregados com outros, existentes na mesma norma, e outros provenientes de outras fontes, para criar-se uma política de segurança adequada à segurança da informação para teletrabalhadores. A exploração desses controles para criar um modelo de segurança da informação para teletrabalhadores é um dos objetivos dessa dissertação, conforme apresentado no Capítulo 5.

3 METODOLOGIA

Este capítulo tem por objetivo apresentar os procedimentos metodológicos utilizados para realização de uma pesquisa de campo.

3.1 Objetivos

Conforme apresentado no Capítulo 1, a questão básica que deverá ser respondida e que sintetiza o problema de pesquisa é: Como gerenciar a segurança da informação em sistemas de teletrabalho?

Como objetivo geral propõe-se uma metodologia para gerenciamento da segurança da informação em sistemas de teletrabalho, que contemple os controles previstos pelas normas de segurança da informação BS7799, ISO/IEC 17799 e NBR ISO/IEC 17799 (Anexo A).

Como objetivos específicos, procura-se:

(a) Apresentar as relações teóricas e empíricas entre segurança da Informação e teletrabalho;
(b) Analisar como as organizações brasileiras que realizam o teletrabalho estão tratando a questão da segurança das informações e
(c) Propor uma metodologia para o gerenciamento da segurança das informações para estas organizações.

No Capítulo 2, através de uma pesquisa bibliográfica, foram apresentadas as relações descritas no item (a).

Como descreve Gil (1991), existem diversos tipos de pesquisa e respectivas formas de execução, tendo-se optado, para analisar a questão identificada no item (b), por uma pesquisa de campo, baseada na aplicação de um questionário, conforme detalhamento realizado neste capítulo.

3.2 Definição de Termos Considerados Importantes para a Pesquisa

Segundo Marconi e Lakatos (2001) a definição com precisão dos termos esclarece e indica o emprego dos conceitos na pesquisa, possibilitando sua investigação e comunicação de forma não-ambígua.

O questionário de pesquisa (Apêndice A) foi elaborado de forma a ser auto-explicativo. As questões trazem entre parênteses o significado dos termos que possam ser desconhecidos pela população em estudo.

A seguir são relacionados os termos que possam suscitar dúvidas de interpretação e suas respectivas definições.

BS7799 e ISO17799: Normas que estabelecem controles de segurança da informação aplicáveis à política de segurança das empresas;

Desktop: Computador de mesa;

Natureza da organização: A constituição jurídica da organização;

Notebook: Computador portátil, próprio para usuários móveis;

Política de Segurança: Documento que descreve as normas e os controles de segurança empregados pela empresa;

Teletrabalho: O trabalho executado a distância através de recursos informáticos e de telecomunicações.

3.3 Delineamento da pesquisa

O estudo desenvolvido nessa pesquisa caracteriza-se como descritivo-analítico, efetivado por meio de em uma abordagem quantitativa de análise. Como descreve Gil (1991), a pesquisa descritiva tem por objetivo estudar as características de um grupo, descrevendo suas variáveis e buscando descobrir possíveis associações entre as mesmas. A pesquisa descritiva assume, em geral, a forma de

levantamento e envolve o uso de técnicas padronizadas de coleta de dados tais como o questionário e a observação sistemática.

Ainda segundo Gil (1991), uma pesquisa pode classificar-se em dois grandes grupos: aqueles que se valem das chamadas “fontes de papel” e aqueles cujos dados são conhecidos por pessoas. No primeiro grupo estão a pesquisa bibliográfica, documental e no segundo, a pesquisa experimental, a pesquisa *ex-post-facto*, o levantamento e o estudo de caso.

Este trabalho se enquadra no segundo grupo, podendo ser mais especificamente definido como um levantamento, ou seja, uma pesquisa que busca a interrogação direta das pessoas cujo comportamento deseja-se conhecer (Gil, 1991).

Segundo Gil, o levantamento desenvolve-se ao longo de várias fases que podem ser definidas na seguinte seqüência, a qual foi rigorosamente considerada na presente pesquisa:

(a) Especificação dos objetivos;
(b) Operacionalização dos conceitos e variáveis;
(c) Elaboração do instrumento para coleta de dados;
(d) Pré-teste do instrumento;
(e) Seleção da amostra;
(f) Coleta dos dados;
(g) Análise e interpretação dos dados e
(h) Apresentação dos dados.

3.4 Coleta de Dados

A estratégia escolhida para responder a pergunta de pesquisa foi a aplicação de um questionário de pesquisa.

O questionário teve por objetivo investigar como as organizações brasileiras estão gerenciando às seguintes questões relacionadas à segurança da informação em sistemas de teletrabalho.

(a) Como os teletrabalhadores acessam remotamente a empresa;

(b) Quais recursos de infraestrutura são fornecidos pela empresa para os teletrabalhadores;
(c) Como os sistemas são monitorados;
(d) Se a política de segurança da empresa contempla o teletrabalho;
(e) Se o teletrabalhador recebe informações e treinamento sobre segurança da informação;
(f) Se a empresa já teve problemas de segurança envolvendo programas de teletrabalho e quais foram eles;
(g) Se as permissões de acesso do teletrabalhador são iguais as dos usuários internos;
(h) Quais são as ferramentas de segurança empregadas pela empresa;
(i) Como é realizado o suporte e a manutenção dos sistemas de teletrabalho e
(j) Qual é o grau de conhecimento e envolvimento da empresa com as normas de segurança BS7799/ISO 17799.

3.4.1 Instrumento para Coleta de Dados

Seguindo as recomendações de Pinto (2001), segundo a qual um questionário de pesquisa não deve ser longo demais para não cansar e desanimar quem está respondendo, foi elaborado um questionário constituído por 21 questões (Apêndice A).

As questões foram dispostas em 3 páginas para evidenciar as características fundamentais das organizações pesquisadas, tais como a natureza e porte econômicos assim como os aspectos relevantes sobre como gerenciam a segurança da informação quanto aos programas de teletrabalho.

As questões de 1 a 20 são de múltipla escolha, ou seja, o informante escolhe sua resposta entre as opções oferecidas. A vigésima primeira questão é aberta, ou seja, o informante pode responder livremente, com frases ou orações, usando linguagem própria e expressando suas opiniões, possibilitando a obtenção de mais informações sobre o assunto, sem prejudicar a tabulação (PINTO, 2001).

Uma folha de rosto foi anexada ao questionário contendo uma apresentação e a descrição do objetivos da pesquisa.

3.4.2 Pré-Teste do Instrumento de Coleta de Dados

Segundo Gil (1991), a validação do instrumento de coleta de dados tem por objetivo garantir que ele meça exatamente aquilo o que se pretende medir.

Para pré-teste do instrumento de pesquisa, foram realizadas duas validações: análise semântica e análise de conteúdo.

Segundo Pasquali (1999), a validação semântica tem por objetivo precípuo verificar se todos os itens de um questionário são compreensíveis para todos os membros da população à qual o instrumento se destina. Na análise de conteúdo, ainda segundo Pasquali, os juízes (avaliadores) devem ser peritos na área do constructo, pois sua tarefa consiste em ajuizar se os itens estão se referindo ou não ao traço em questão.

Para validação semântica, o questionário foi aplicado em caráter de teste para duas turmas de 30 alunos do curso *de Tecnologia de Redes de Computadores*, de uma faculdade localizada em Brasília (DF), perfazendo um total de 60 questionários aplicados. Foi solicitado aos alunos que assinalassem e descrevessem quaisquer questões ou partes do questionário que não fossem claramente compreendidas. Após a análise dos questionários devolvidos, com os respectivos apontamentos, pequenas correções foram realizadas e um texto explicativo foi acrescentado ao início do questionário.

Para validação do conteúdo, o questionário, em sua forma definitiva, foi apresentado para apreciação por cinco profissionais da área de segurança da informação, todos com nível de escolaridade de pós-graduação e atuando profissionalmente nessa área. Foi solicitado a esses profissionais que procurassem identificar a adequação e conteúdo de cada questão, apontando falhas, incoerências ou insuficiência das mesmas. Não foram necessárias correções no instrumento após essa validação, dando-se, portanto, como concluída a fase de elaboração.

3.4.3 População e Amostragem

Foi decidido realizar-se um levantamento por meio de amostragem. A escolha desse método deve-se à natureza da situação alvo, envolvendo programas e sistemas de teletrabalho com características potencialmente similares em face das soluções e práticas de segurança hoje disponíveis no mercado.

Por não existirem estatísticas, até o presente momento, sobre quais são as populações de teletrabalhadores e de empresas que mantêm programas de teletrabalho no Brasil, para a realização dessa pesquisa, optou-se for efetuar uma amostragem não probabilística intencional.

Na amostragem probabilística, os resultados obtidos podem ser projetáveis para a população total ao passo que na amostragem não probabilística, o pesquisador usa seu julgamento para selecionar os membros da população que são boas fontes de informação precisa, sem, contudo, poder generalizar os resultados obtidos (OLIVEIRA, 2001).

Para responder a pergunta de pesquisa foi definido que o universo a ser pesquisado seria formado por empresas, organizações públicas ou privadas que empreguem teletrabalhadores formais ou informais e que atuem no território brasileiro.

A amostra foi definida intencionalmente, selecionando-se empresas que mantinham programas de teletrabalho formal ou informalmente. O acesso às empresas foi obtido solicitando o preenchimento do questionário de pesquisa aos funcionários das mesmas, presentes em:

(a) Cursos de graduação e pós-graduação na área de informática em faculdades de Brasília, DF;
(b) Cursos de informática extracurriculares realizados em São Paulo, SP e
(c) Listas de discussão na Internet *BOS* (Best Of Security Brazil – vinculada ao site www.securenet.com.br) e *Network Designers,* (vinculada ao site www.networkdesigners.com.br), sendo a primeira relativa à segurança da informação e às segunda à redes de computadores.

A escolha de teletrabalhadores da área de informática teve por objetivo facilitar a realização da pesquisa uma vez que esses profissionais, devido à natureza de suas atividades, normalmente têm conhecimento das questões envolvendo segurança da informação em suas organizações.

Os participantes da pesquisa, na condição de empregados das empresas, foram representantes das opiniões dos seguintes grupos:

(a) Gerentes e Supervisores de Informática;
(b) Equipe de Segurança da Informação;
(c) Consultores da área de tecnologia da informação e
(d) Empregados da área de informática em geral.

3.4.4 Coleta dos Dados

Todos os participantes foram convidados a contribuir com a pesquisa, preenchendo voluntariamente os questionários.

A pesquisa abrangeu o processamento de 46 questionários enviados a teletrabalhadores que atuam na área de informática, realizada entre julho e outubro de 2001.

A entrega dos questionários de pesquisa foi feita pessoalmente pelo pesquisador ou por meio de correio eletrônico, sendo o entrevistado, nesse último caso, contatado previamente, seja por telefone, correio eletrônico ou pessoalmente, com objetivo de obter sua anuência para o envio do questionário.

O questionário de pesquisa impresso foi entregue aos teletrabalhadores localizados entre alunos de cursos de graduação e pós-graduação da área de informática, em faculdades de Brasília, DF. A versão eletrônica do questionário foi enviada aos teletrabalhadores participantes das listas de discussão na Internet *BOS* (Best Of Security Brazil – vinculada ao *site* www.securenet.com.br) e *Network Designers,* (vinculada ao *site* www.networkdesigners.com.br), sendo a primeira relativa à segurança da informação e a segunda às redes de computadores. O envio do questionário por meio de correio eletrônico foi precedido por um anuncio nas listas solicitando que os teletrabalhadores presentes manifestassem seu interesse em participar da pesquisa.

Os questionários preenchidos foram recolhidos pessoalmente pelo pesquisador ou enviados pelos respondentes por meio de correio eletrônico.

Os questionários enviados por correio eletrônico foram editados em Microsoft Word 97 por este ser o processador de textos mais empregado no país, reduzindo assim a possibilidade de incompatibilidade de formatos.

3.5 Análise dos Dados

A análise dos dados caracteriza-se como uma análise estatística dos resultados obtidos, sendo apresentada em detalhes no Capítulo 4.

3.6 Limitações da Pesquisa

Os resultados da pesquisa não podem ser generalizados para todas as organizações brasileiras, pelos seguintes motivos:

(a) Foi adotada uma amostragem não probabilística da população alvo;
(b) A maioria das empresas pesquisadas são, sob o ponto de vista econômico e financeiro, de grande porte. Empresas de médio e pequeno porte podem apresentar características distintas da amostra pesquisada;
(c) A maioria das empresas pesquisadas encontram-se em Brasília, DF e
(d) Pelo fato da pesquisa ter sido realizada em um momento específico de tempo, os resultados refletem a realidade atual que podem não mais ser verdadeiros no futuro.

4 APRESENTAÇÃO E ANÁLISE DOS DADOS

Este capítulo tem por objetivo apresentar os dados obtidos através do levantamento descrito no Capítulo 3. Para facilitar a compreensão dos aspectos dessa investigação, os resultados são descritos seqüencialmente, conforme se apresentam no questionário de pesquisa (Apêndice A).

O questionário foi entregue e recolhido pessoalmente pelo pesquisador ou foram encaminhados e devolvidos por correio eletrônico.

No primeiro caso, todos os questionários, num total de 26, foram entregues e recolhidos pessoalmente. Foram também enviados 16 questionários por correio eletrônico para teletrabalhadores de diferentes empresas, dos quais 9 foram devolvidos.

Dos questionários devolvidos por correio eletrônico, um não pode ser aproveitado por estar em formato irreconhecível pelos editores de texto disponíveis. Excluindo-se os questionários irrecuperáveis e aqueles que se referiam a mesma empresa, totalizou-se 25 questionários válidos para análise.

4.1 Caracterização dos Respondentes

As questões de um a quatro do questionário objetivam caracterizar os respondentes e as empresas em que trabalham.

Com relação à área de atuação dos respondentes, 84% informaram trabalhar na área de informática. Tal resultado era esperado, em virtude da amostra ter sido intencional (Capítulo 3). No que diz respeito à área geográfica de atuação da empresa, 20% das empresas têm atuação regional, 36% têm atuação nacional e 44% têm área de atuação internacional. Esses índices indicam que o teletrabalho encontra-se disseminado no meio empresarial, não se concentrando, por exemplo, em empresas estrangeiras que podem, eventualmente, deter maior *know-how* administrativo e tecnológico do que as empresas nacionais.

No quesito referente ao estado do Brasil onde estão localizadas as empresas e os respondentes, a tabela 4.1 demonstra os resultados obtidos.

Tabela 4.1: Localização das Empresas Pesquisadas

Estado	%	Nº Questionários
Distrito Federal	48	12
São Paulo	32	8
Rio de Janeiro	8	2
Bahia	4	1
Ceará	4	1
Maranhão	4	1
Total	100	25

Esta distribuição se justifica pelo fato da pesquisa ter se concentrado em Brasília, DF, onde os questionários foram entregues pessoalmente aos respondentes sendo os demais, localizados em outros estados, alcançados apenas por meio de correio eletrônico.

No que tange à natureza da organização, ou seja, sua classificação quanto ao capital, 36% das empresas são multinacionais, 32% são privadas brasileiras, 24% são órgãos públicos, 4% são empresas de economia mista, e 4% são associações, sindicatos, organizações não governamentais (ONGs) ou assemelhadas. Conforme pode ser observado na tabela 4.2, esses resultados demonstram a predominância de empresas privadas como usuárias de programas de teletrabalho.

Tal resultado pode ser explicado pela necessidade dessas empresas em empregar formas não tradicionais de administração do trabalho de forma a aumentar sua competitividade (MELLO, 1999).

Tabela 4.2: Natureza das Empresas Quanto ao Capital

Empresas	%
Multinacionais	36
Privadas brasileiras	32
Órgão públicos	24
Economia mista	4
Associações ou sindicatos	4
Total	100

4.2 Relações das Empresas com os Teletrabalhadores

Para aprofundar o conhecimento sobre o teletrabalho, a quinta questão do questionário procura identificar qual é a experiência da empresa com o teletrabalho e a sexta questão procura identificar em que área da empresa encontram-se os teletrabalhadores.

A grande maioria (80%), informou que a empresa tem teletrabalhadores. Cerca de 16% informaram que a empresa já teve teletrabalhadores no passado mas não no presente. Cerca de 4%, ou seja, um respondente, informou que a empresa estava estudando ou implantando um programa de teletrabalho (Tabela 4.3).

Tabela 4.3: Experiência das Empresas com Teletrabalho

Experiência	%
Tem teletrabalhadores	80
Teve teletrabalhadores	16
Em estudo	4
Total	100

Esses resultados reforçam as expectativas da pesquisa, uma vez que os respondentes foram previamente selecionados quanto a existência de programas de teletrabalho em suas empresas antes de receberem o questionário de pesquisa.

Quanto a área de atuação do teletrabalhador na empresa, apenas 6 respondentes (24%) assinalaram uma única opção. Um total de 13 respondentes (52%) informaram que os teletrabalhadores encontram-se na diretoria da empresa. Destes, 12 (48%) também informaram que os teletrabalhadores encontram-se na gerência e na área de informática da empresa. No total, os teletrabalhadores que fazem parte da área de informática totalizaram 72% dos 25 respondentes. Um total de 24% dos respondentes informaram ter teletrabalhadores na área comercial e, por fim, 32% informaram ter teletrabalhadores em outras. Apenas 2 respondentes (8%) informaram ter teletrabalhadores em todas as áreas relacionadas no questionário.

O fato de vários respondentes pertencerem à área de informática, onde exercem função gerencial, significa que suas respostas à sexta questão podem

refletir sua situação pessoal, inflacionando o número de teletrabalhadores que atuam na área gerencial da empresa, como mostra a tabela 4.4:

Tabela 4.4: Área de Atuação dos Teletrabalhadores

Área	%
Informática	72
Diretoria	52
Gerência	48
Comercial	24
Outras	32

4.3 Como os Teletrabalhadores acessam as Empresas

As questões 7, 8 e 9 do questionário têm por propósito verificar como os teletrabalhadores acessam à rede da empresa e quais recursos são fornecidos pela mesma.

Para 28% dos respondentes o acesso à rede da empresa é feito exclusivamente por meio de microcomputadores *desktop* (de mesa), instalados em suas residências e para 16% dos respondentes o acesso é feito exclusivamente por meio de microcomputadores *notebooks* (computadores portáteis, móveis). Para a grande maioria (56%), contudo, o acesso é feito empregando-se tanto computadores *desktop* quanto *notebooks.*

Uma hipótese para explicar a disponibilidade de mais de um computador para acesso por parte da maioria dos teletrabalhadores seria o fato de muitos dos respondentes ocuparem cargos nas áreas de direção e gerência (conforme demonstrado no item 4.3) onde poderia haver maior dotação de recursos de todos os tipos no intuito de maximizar a produtividade dos executivos.

Com relação ao canal de comunicação de dados, 76% dos respondentes informaram que o acesso é realizado por meio de linha telefônica discada e 24% por meio de banda larga, ou seja, uma conexão de alta velocidade empregando um *Cable Modem, DSL Modem* ou outra tecnologia. Oito por cento dos respondentes informaram que empregam ambos canais de comunicação, pelo fato dos mesmos

realizarem seus acessos tanto por meio de microcomputadores *desktop* quanto por meio de *notebooks*. Cabe ressaltar que os dados obtidos estão de acordo com a realidade atual do mercado brasileiro de acesso a canais de banda larga. Trata-se de um serviço de custo elevado e restrito a poucas regiões, existindo hoje apenas 400 mil usuários de banda larga no Brasil (BALIEIRO, 2001), o que obriga a maioria dos teletrabalhadores a empregar linhas comutadas.

Quanto ao fornecimento de infraestrutura por parte das empresas para os teletrabalhadores efetuarem seus acessos, 16% informaram que as empresas fornecem microcomputadores desktop, 72% fornecem microcomputadores *notebooks*, 64% fornecem os *softwares* aplicativos, 36% fornecem periféricos, 60% fornecem acesso à Internet e, em apenas 8% dos casos, a empresa não fornece nenhum dos itens necessários ao acesso.

A tabela 4.5, apresentada a seguir, sintetiza os dados referentes a infra-estrutura.

Tabela 4.5: Fornecimento de Infraestrutura para os Teletrabalhadores

Infraestrutura	**%**
Microcomputadores notebooks	72
Microcomputadores desktop	16
Softwares aplicativos	64
Periféricos	36
Acesso a Internet	60
Nenhuma	8

Os resultados apontam para a predominância do uso dos microcomputadores *notebooks*, provavelmente devido a sua facilidade de transporte, que permite seu emprego na empresa, no lar do teletrabalhador ou em trânsito. O emprego de *notebooks* também facilita o suporte, manutenção e verificação dos mesmos, uma vez que podem facilmente ser levados aos departamentos encarregados de suporte e manutenção. Contudo, o emprego de *notebooks* é potencialmente perigoso com relação à segurança da informação, conforme mencionado no Capítulo 2, pois podem ser facilmente roubados e terem suas informações acessadas (FBI, 2001).

4.4 Política de Segurança Aplicada ao Teletrabalho

As questões de 10 a 17 têm por objetivo investigar como a empresa trata a questão da segurança da informação com relação a seus programas de teletrabalho.

Com relação ao ambiente de trabalho do teletrabalhador, ou seja, em sua residência, 8% dos respondentes informaram que a empresa faz vistorias periódicas no mesmo. Cerca de 8% informaram que a empresa faz vistorias periódicas apenas no computador do teletrabalhador. Um total de 24% informaram que a empresa monitora suas atividades a distância, empregando ferramentas de gerenciamento. Por fim 60% dos respondentes, ou seja, a grande maioria, informou que a empresa não realiza vistorias ou monitoração do ambiente do computador ou das atividades do teletrabalhador.

Esses resultados apontam para um alto percentual de empresas que ainda não atentou para os riscos inerentes às atividades de teletrabalho para com segurança da informação de seus sistemas de TI.

É possível que essas empresas mantenham apenas procedimentos de segurança da informação informais e restritos, sendo, portanto, pouco seguros.

Tabela 4.6: Ações da Empresa com relação às Atividades do Teletrabalhador

Ações da Empresa	%
Não faz vistoria ou monitoração	60
Monitoração a distância	24
Faz vistorias na residência do teletrabalhador	8
Faz vistorias no computador do teletrabalhador	8
Total	100

Esses percentuais estão em conformidade com *o Global Information Security Survey 2001*[(1)], que, ao pesquisar 4462 empresas em todo mundo, constatou que somente 31% das empresas possuem objetivos de segurança por escrito e apenas

[(1)] Levantamento Segurança da Informação Global 2001

19% possuem uma descrição completa de procedimentos, e a grande maioria (43%) limita-se a procedimentos informais de segurança. Na América do Sul esse percentual seria pouco menor, situando-se na casa dos 38% (SCAGLIA, 2001).

Na questão referente à política de segurança, apenas 36% dos respondentes informaram que as políticas de suas empresas tratam especificamente a questão do teletrabalho, sendo que, a grande maioria, 60% informaram que as políticas não tratam a questão. Um respondente não soube dar essa informação.

Ainda com relação à política de segurança da empresa, 44% dos respondentes informaram que os teletrabalhadores são oficialmente informados pela empresa acerca de sua política de segurança, ao passo que 52% informaram não receber essa informação. Cerca de 4%, ou seja, um respondente, não soube informar se a empresa divulgava a política de segurança, o que parece indicar uma resposta negativa quanto a essa questão, o que elevaria o índice para 56%.

Tabela 4.7: Divulgação da Política de Segurança na Empresa

Ação da Empresa	**%**
Não divulgou a política de segurança para os teletrabalhadores	52
Divulgou a política de segurança para os teletrabalhadores	44
Os teletrabalhadores não souberam informar	4
Total	100

No que tange ao treinamento dos teletrabalhadores, 36% dos respondentes informaram que a empresa fornece treinamento específico sobre segurança da informação para teletrabalhadores, sendo que 60%, ou seja, a maioria das empresas, não fornecem esse tipo de treinamento.

Esses dados, sintetizados na tabela 4.8, demonstram que a maioria das organizações precisam aumentar seus esforços com relação à segurança da informação de um modo geral e não apenas no que diz respeito aos teletrabalhadores.

Tabela 4.8: A Política de Segurança Utilizada pelas Empresas Pesquisadas

Atividades Relativas à Segurança da Informação	%
Vistoria periódica à residência do teletrabalhador	8
Vistoria periódica no computador do teletrabalhador	8
Monitoração a distância do teletrabalhador	24
Política de segurança abrangendo o teletrabalho	36
Treinamento quanto à segurança da informação	36

Quanto a possíveis problemas envolvendo a segurança de informação na organização e seus teletrabalhadores, 64% dos respondentes informaram que a empresa nunca teve problemas dessa natureza, contra 16% que informaram que sim, a empresa teve problemas dessa natureza mas, mesmo assim, manteve seu programa de teletrabalho. Não houve casos onde, devido a problemas com segurança da informação, a empresa tenha encerrado o programa de teletrabalho ou ainda empresas que não tenham implantado um programa de teletrabalho em virtude dos riscos envolvidos. Apenas 4%, ou seja, um respondente, informou que a empresa não implantou o teletrabalho diante dos riscos. Oito por cento informaram que as empresas, apesar de não terem apresentado problemas relativos à segurança da informação, resolveram encerrar seus programas de teletrabalho diante dos riscos envolvidos. A tabela 4.9 sintetiza os dados obtidos:

Tabela 4.9: Ocorrência de problemas de segurança da informação no programa de teletrabalho e a reação das empresas

Ocorrências	%
Nunca teve problemas com o programa de teletrabalho	64
Teve problemas mas decidiu manter o programa	16
Nunca teve problemas mas encerrou o programa	8
Não responderam	8
Não implantou o programa devido aos riscos	4
Total	100

No que diz respeito ao controle de acesso remoto à rede da empresa, 52% dos respondentes informaram que o teletrabalhador tem as mesmas permissões de acesso que um usuário da rede interna, ao passo que 44% têm um acesso mais restrito, menor que um usuário da rede interna. Um respondente (4%), desconhecia a forma como era feito o controle de acesso.

Esses resultados demonstram que cada empresa aborda diferentemente o problema do nível de acesso, uma vez que devem ser levados em conta a análise de riscos, os mecanismos de segurança empregados e, por fim, a necessidade de acesso ao sistema de TI da empresa por parte dos teletrabalhadores.

Para finalizar este tópico, a décima sétima questão verifica quais ferramentas de segurança são empregadas pelas organizações para atender a seus programas de teletrabalho. Os principais tipos de ferramentas hoje existentes no mercado nacional e internacional, descritas no Capítulo 3, foram relacionadas no questionário, sendo os resultados obtidos apresentados na tabela 4.10.

Tabela 4.10: Ferramentas de Segurança Utilizadas pelas Empresas

Ferramentas	**%**
Firewall Corporativo	68
Firewall Pessoal	20
Anti-Vírus na Rede Interna	64
Anti-Vírus no computador do Teletrabalhador	68
IDS	32
Criptografia de Arquivos	36
Criptografia das Comunicações (sem ser VPN)	8
VPN	32
PKI	4
Call-Back	20
Servidor RADIUS	48
Biometria	4
Token Card	8
Logs e Auditoria	4
Outros	44

Como demonstram os dados, da Tabela 4.9, os itens mais relevantes apontados pelas empresas pesquisadas são o *Firewall* corporativo e o anti-vírus, instalados tanto no computador do teletrabalhador quanto na rede interna. Tais resultados estão em consonância com outros levantamentos que demonstram a predominância dessas mesmas ferramentas nas empresas de um modo geral (FBI, 2001).

O emprego de criptografia, VPN, *Logs* e Auditoria é expressivo, assim como o uso de servidores RADIUS, esse último capaz de controlar com eficiência o acesso dos teletrabalhadores à rede interna.

O emprego das demais ferramentas demonstrou ser bem reduzido. Tal fato pode ser explicado pela sua complexidade com relação à implementação (IDS) e gerenciamento (PKI), ou ainda por não estarem bem disseminadas (Biometria).

Causa surpresa a constatação de que poucos teletrabalhadores empregam *Firewall* pessoal em seus computadores. Tal ferramenta, de fácil obtenção, inclusive de forma gratuita na Internet, é essencial para impedir invasões e outros tipos de ataques aos computadores pessoais. Provavelmente a causa de sua pouca utilização está no desconhecimento dos teletrabalhadores e no descuido da empresas para esse ponto.

Por fim, com relação ao suporte e manutenção dos sistemas dos teletrabalhadores, composto pelo *hardware* (computadores) e *software* (sistema operacional e aplicativos), 68% dos respondentes informaram que o suporte é prestado por funcionários da empresa, 8% por prestadores de serviços credenciados pela empresa e 24% informaram que o suporte e a manutenção são responsabilidade do teletrabalhador, o que implica a transferência de grande parte da responsabilidade com relação à segurança da informação para esse último, com um conseqüente aumento do risco para a empresa.

4.5 Relação com a Norma ISO/DIS 17799

A décima oitava e a décima nona questão têm por objetivo avaliar qual é o grau de conhecimento e envolvimento do respondente e da empresa com a norma ISO/DIS 17799 ou com sua predecessora, a BS7799.

Um total de 56% dos respondentes informaram que ainda não conheciam a norma e 40% informaram já conhecê-la superficialmente. Apenas 4%, ou seja, um respondente, informou conhecer bem a norma. Com relação às empresas, 72% das mesmas ainda não tomaram formalmente conhecimento da mesma, 20% estão avaliando a norma, 4% estão implantando-a e apenas uma empresa (4%) já concluiu esse processo. Nenhuma das empresas pesquisadas obteve a certificação correspondente.

Tais resultados podem ser explicados pelo fato das normas ISO/DIS 17799 e BS7799 terem sido criadas e homologadas a relativamente pouco tempo, carecendo, portanto, de maior divulgação junto aos profissionais e empresas.

4.6 Problemas com Segurança da Informação e Teletrabalho Relatados

A vigésima primeira questão foi criada com o propósito de oferecer a oportunidade dos respondentes indicarem problemas específicos que tenham enfrentado em seus programas de teletrabalho no que se refere à segurança das informações. Cerca de 20% dos questionários apontaram respostas a esta questão, conforme descrito a seguir:

Problemas enfrentados:

(a) Desconhecimento das normas (identificado por 8% dos respondentes);
(b) Falta de uma política de segurança na empresa (identificado por 12% dos respondentes) e
(c) Dificuldade em conciliar os interesses dos teletrabalhadores que ocupam cargos de diretoria com a necessidade de se estabelecer controles de acesso remoto mais restritos (identificado por 4% dos respondentes).

Soluções empregadas

(a) Necessidade de padronização dos sistemas operacionais para padronizar procedimentos de segurança;

(b) Criação e manutenção de uma equipe de profissionais de segurança da informação;
(c) Realização de testes periódicos para avaliar a vulnerabilidade do sistema e
(d) Manutenção de um pequeno número de teletrabalhadores para restringir o risco.

4.7 Convite à Avaliação de uma Metodologia de Segurança para Teletrabalho

Por fim, a vigésima questão teve por objetivo verificar o interesse dos respondentes ou de suas empresas em avaliar uma metodologia de segurança da informação para teletrabalho. Um total de 80% dos respondentes manifestaram interesse em avaliar uma metodologia desse tipo. A proposta dessa metodologia é apresentada nessa dissertação, no Capítulo 5.

Tabela 4.11: Convite à Avaliação de uma Metodologia de Segurança para Teletrabalho

Interesse	%
Sim	80
Não	20

4.8 Conclusão

O questionário de pesquisa avaliou diversos aspectos do emprego do teletrabalho nas empresas, especialmente com relação a pontos envolvendo a segurança das informações.

Com a finalidade de tornar mais claro o entendimento e apreensão dos resultados dessa pesquisa, na tabela 4.12, apresentada a seguir, são destacados os resultados obtidos, agrupados com relação aos itens computados predominantes.

Tabela 4.12: Resumo dos Resultados da Pesquisa

Resumo	%
Empresas que têm atuação nacional ou internacional	80
Empresas localizadas em Brasília, DF	48
Empresas privadas, nacionais ou multinacionais	68
Empresas que têm teletrabalhadores no momento	80
Respondentes que trabalham na área de informática	72
Acesso à empresa por meio de rede pública de telefônica	76
Empresas que fornecem computadores aos teletrabalhadores	88
Empresas que não vistoriam o ambiente do teletrabalhador	60
Empresas que não abordam o teletrabalho na política de segurança	60
Empresas que não treinam os teletrabalhadores quanto à segurança	60
Empresas sem histórico de problemas de segurança X teletrabalho	64
Empresas que restringem o nível acesso dos teletrabalhadores	44
Empresas que fornecem suporte e manutenção aos teletrabalhadores	68
Empresas que ainda desconhecem a norma ISO/DIS 17799	72

A maior parte das empresas pesquisadas informaram empregar as ferramentas de segurança mais tradicionais e mais largamente disseminadas: *Firewall* Corporativo e Anti-vírus.

Apesar de empregarem essas ferramentas e outros meios para garantir a segurança de seus sistemas, 80% dos respondentes demonstraram interesse em avaliar uma metodologia de segurança da informação para teletrabalho, demonstrando assim a constante preocupação em buscar novas formas de se protegerem, fazendo frente aos desafios de assegurar a confidencialidade, integridade e disponibilidade de suas informações.

5 UM MODELO DE SEGURANÇA DA INFORMAÇÃO PARA O TELETRABALHO

Este capítulo apresenta um modelo de segurança, criado com o objetivo de possibilitar o estabelecimento de um programa de teletrabalho que contemple a segurança das informações de forma rápida e eficiente e que facilite seu posterior gerenciamento.

5.1 Introdução

Conforme descrito no Capítulo 2, a segurança da informação é hoje uma necessidade fundamental para grande parte das organizações, aplicando-se a inúmeras atividades, inclusive ao teletrabalho.

Embora seja relativamente fácil implantar medidas de segurança para o acesso remoto e incorporá-las à política de segurança da empresa, a maioria dos autores, tal como Nilles (1997), Trope (1999), Mello (1999) e Leonhard (1995) abordam a questão de forma superficial ou incompleta, atendo-se a pontos específicos. Geralmente a literatura aborda essa questão focalizando a implementação de algumas ferramentas ou procedimentos de segurança (CONNOR, 2000; MOUSTAFA, 2000; YASIN, 2000) sem oferecer uma visão de conjunto do problema.

Dentre as abordagens sistêmicas da questão da segurança da informação, destaca-se a norma ISO/DIS 17799 que fornece um conjunto de controles criados especificamente para promover a segurança da informação para o teletrabalho. As organizações contam hoje, portanto, com as seguintes opções para implementar uma política de segurança para um programa de teletrabalho:

(a) Implementar medidas de segurança tradicionais para acesso remoto;
(b) Instalar um sistema proprietário de segurança fornecido pela indústria;
(c) Aplicar um *chekli*st [1]de segurança disponível na Internet;

[1] Lista de verificação de conformidade.

(d) Contratar uma empresa de consultoria para implantar o programa e
(e) Aplicar os controles da norma de segurança ISO 17799.

Por não abordarem a questão como um todo, a aplicação de qualquer uma dessas opções, por si só, pode ser insuficiente para garantir a segurança das informações.

Constata-se, portanto, a necessidade de um modelo de segurança que possibilite implantar e manter um nível de integridade, disponibilidade e confidencialidade das informações, senão ideal, pelo menos satisfatório ante às ameaças e riscos para o programa. É necessário também que esse modelo possibilite uma visão global e que proporcione uma abordagem completa da questão, como demonstra a figura 5.1.

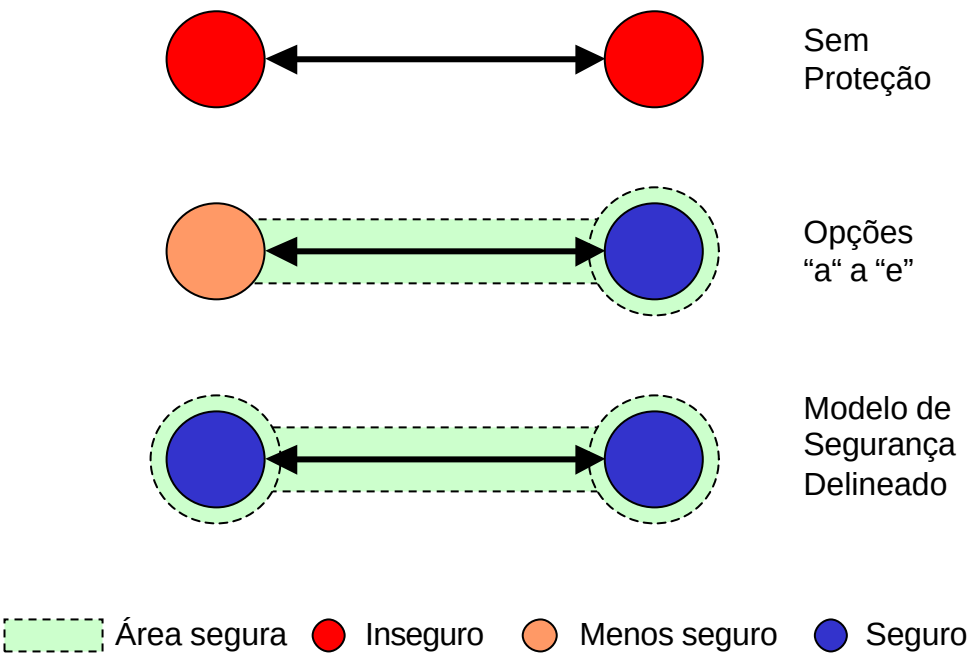

Figura 5.1: Opções de Segurança para o Teletrabalho

Os primeiros modelos de segurança da informação surgiram nos anos 70 (DENNING, 1999). O termo *modelo de segurança* tem sido usado para descrever qualquer definição formal com relação a requisitos de confidencialidade, integridade e disponibilidade da informação.

Na literatura referente à segurança da informação, existem dois tipos distintos de modelos de confidencialidade: em termos mais limitados, modelo de segurança especifica um mecanismo particular de reforço da confidencialidade baseado no controle de acesso e, em termos mais amplos, modelo de segurança especifica os requisitos de confidencialidade para sistemas (McLEAN, 1994).

A seguir, é apresentado um modelo de segurança no sentido amplo, com objetivo de assegurar, além da confidencialidade, a integridade e a disponibilidade das informações em um sistema de teletrabalho.

5.2 Requisitos de um Modelo de Segurança da Informação para Teletrabalho

Com base nos fatores necessários para um gerenciamento efetivo da segurança da informação em um sistema de teletrabalho, conforme descrito no capítulo 2, estabeleceram-se os requisitos que um modelo de segurança para teletrabalho deve apresentar para assegurar as informações:

- Deve ser baseado em padrões reconhecidos de segurança da informação;
- Deve proporcionar um nível de segurança adequado aos riscos;
- Deve atender a diferentes requisitos de segurança;
- Deve abranger os aspectos lógico, físico e pessoal da segurança da informação;
- Deve incluir medidas de recuperação de falhas e desastres;
- Dever ser validado;
- Deve ser permanentemente atualizado;
- Deve fazer parte do modelo e da política de segurança da informação da empresa e
- Deve contar com a participação e comprometimento do teletrabalhador.

5.3 O Modelo Proposto

Com base nos requisitos especificados no item 5.2, delineou-se um modelo de segurança da informação aplicável a sistemas de teletrabalho residencial ou

móvel, sendo esse último baseado em computadores portáteis (laptops/notebooks), fundamentado nas recomendações e controles da norma ISO 17799.

Com esse modelo, procurou-se facilitar o processo de implantação e gerenciamento da segurança da informação em organizações que desejem manter programas de teletrabalho.

O modelo proposto consiste nos componentes descritos a seguir e detalhados ao longo deste capítulo.

(a) Um fluxograma de aplicação. Informa quais são as fases a serem seguidas para a implantação do modelo na empresa;
(b) Uma classificação da segurança da informação em níveis. Possibilita uma escolha das ferramentas de segurança necessárias de forma simples e rápida;
(c) Uma metodologia para análise de riscos. Possibilita o enquadramento dos riscos e vulnerabilidades para o sistema em um dos níveis de segurança do modelo;
(d) Controles de segurança recomendáveis e obrigatórios. Possibilitam criar uma política de segurança eficiente para manutenção da segurança da informação do sistema de teletrabalho e
(e) Um modelo de arquitetura de segurança. Descreve uma arquitetura de segurança básica para o sistema.

5.3.1 Aplicação do Modelo

A aplicação obedece às recomendações preceituadas pela norma ISO/DIS 17799, começando pela análise de riscos e o enquadramento do sistema necessário em um dos três Níveis de Segurança.

A implantação do modelo de segurança em uma organização pode ser dividida em três fases:

1ª Fase – Planejamento: análise de riscos, classificação do nível de segurança necessário e aplicação dos controles de segurança;

2ª Fase – Implementação: implementação das ferramentas de segurança, montagem, configuração, testes e validação dos sistema e

3ª Fase – Gerenciamento: treinamento, auditorias e reavaliações periódicas do sistema.

A figura 5.2, apresentada a seguir, mostra o fluxograma de aplicação do modelo de segurança proposto.

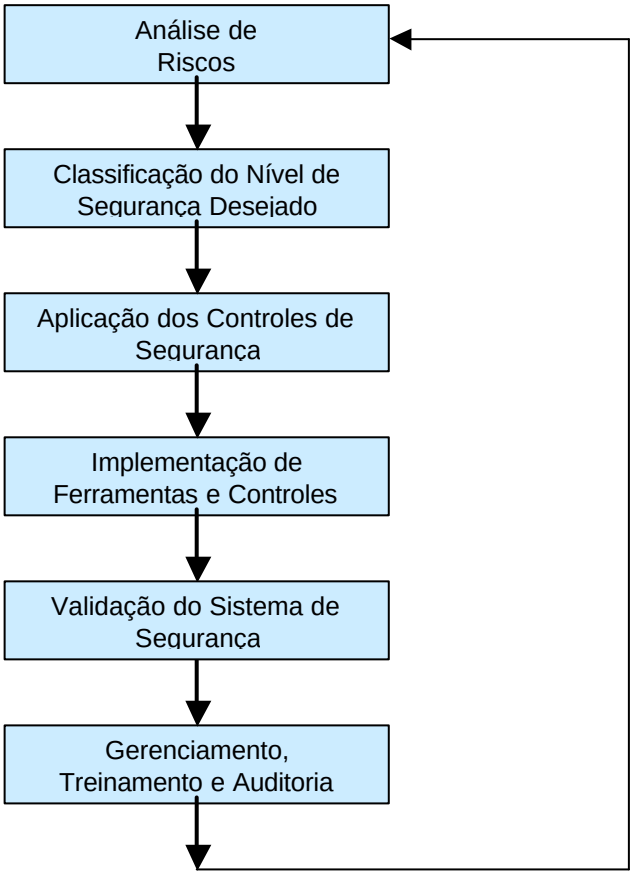

Figura 5.2: Fluxograma de Aplicação do Modelo de Segurança

5.3.2 Níveis de Segurança

Com a finalidade de atender a necessidades diversificadas de acesso e segurança, diversos sistemas de classificação, tal como o *Orange Book* e o *Common Criteria* foram criados, onde essas necessidades são atendidas através da

implementação de vários níveis de segurança, partindo-se de níveis menos seguros até alcançar níveis mais seguros (BRYDEN, 2001).

Dessa forma, com base no fato de que as necessidades de segurança variam de empresa para empresa e também considerando os custos de implementação e gerenciamento, foram definidos três níveis de segurança para o modelo, de forma a equacionar às necessidades das diversas empresas:

(a) **Nível de Segurança 1:** nível básico de segurança;
(b) **Nível de Segurança 2:** acréscimo de certificação digital, *Call-back* e IDS e
(c) **Nível de Segurança 3:** acréscimo de outras ferramentas de segurança.

Os níveis são dispostos em camadas como mostra a figura 5.3, cada qual consistindo na implementação progressiva de ferramentas e procedimentos tanto no computador do teletrabalhador, quanto na empresa, como mostra o Quadro 5.2.

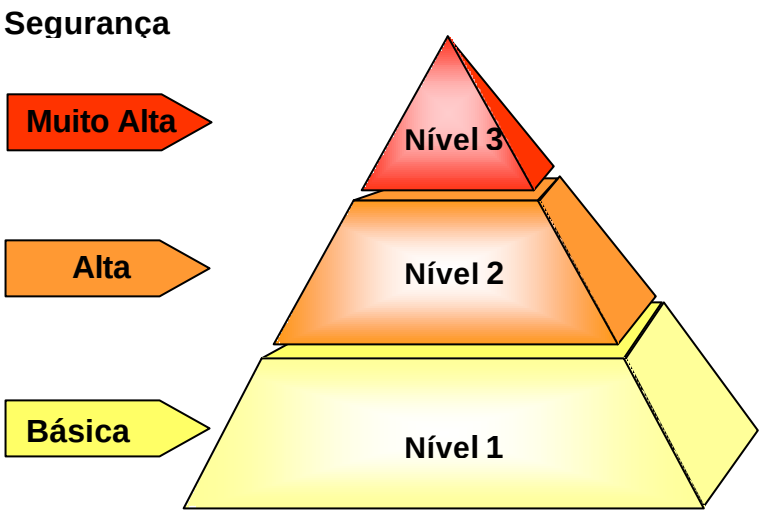

Figura 5.3: Níveis de Segurança do Modelo

O Nível de Segurança 1 é básico. As ferramentas de segurança designadas são aplicáveis, obrigatoriamente, a todos os casos de teletrabalho, exigindo uma arquitetura de segurança simples na empresa, composta basicamente por um *firewall* corporativo. A segurança é garantida pela presença de um *firewall* e um anti-vírus na empresa e no computador do teletrabalhador assim como pelo uso de uma VPN para assegurar a autenticação e a confidencialidade das comunicações.

O Nível de Segurança 2 é aplicável aos casos de teletrabalho onde o valor das informações e o grau de risco justificam maior investimento financeiro e operacional, exigindo, além dos itens especificados para o Nível 1, uma arquitetura de segurança complexa na empresa, empregando, por exemplo, uma DMZ (Demiliteried Zone – Zona Desmilitarizada) para disponibilização de serviços pouco seguros, um sistema de detecção de intrusos (IDS) e certificação digital.

Por fim, o Nível de Segurança 3 é aplicável aos casos de teletrabalho onde o valor das informações e o grau de risco justificam a aplicação de ferramentas extras de forma a maximizar a segurança, principalmente no aspecto da segurança física, envolvendo um custo maior de implementação e gerenciamento, além de incorporar os itens especificados para os Níveis 1 e 2. A arquitetura de segurança poderá ser mais complexa do que a do Nível 2, empregando, por exemplo, mais de um *firewall* entre a rede interna e a rede externa.

O quadro 5.1, apresentado a seguir, resume as características e aplicações de cada nível de segurança.

Quadro 5.1: Aplicação dos Níveis de Segurança

NÍVEL DE SEGURANÇA	SEGURANÇA PROPORCIONADA	APLICAÇÃO
3	Muito Alta	Organizações Militares Comunidades de Inteligência Organizações Policiais
2	Alta	Organizações Governamentais Bancos Instituições Financeiras Teletrabalhadores móveis Suporte Remoto ao Sistema.
1	Básica	Empresas públicas e privadas; Organizações com baixo índice de riscos e ameaças

O Quadro 5.2, apresentado a seguir, detalha quais ferramentas devem ser empregadas em cada Nível de Segurança, tanto na empresa como nas instalações do teletrabalhador.

No Nível de Segurança 1, todas as ferramentas relacionadas são de uso obrigatório. Essas ferramentas são de uso mais freqüente e, portanto, de mais fácil implementação, uma vez que existem muitos fornecedores e pessoal habilitado para sua instalação, configuração e gerenciamento. O *Backup* dos dados do teletrabalhador pode ser feito no computador deste ou no servidor da empresa. Nesse nível, não existe grande diferença entre um sistema de teletrabalho e uma típica Intranet corporativa.

Quadro 5.2: Especificações dos Níveis de Segurança

NÍVEL DE SEGURANÇA 1 [Ferramentas de Uso Obrigatório]	
Computador do Teletrabalhador	**Empresa**
Firewall Pessoal VPN ou SSL/SSH Anti-vírus Backup Criptografia de arquivos sensíveis em laptops Estabilizador de Tensão ou No-Break	Firewall Corporativo VPN ou SSL/SSH Anti-vírus Backup Arquitetura de segurança simples
NÍVEL DE SEGURANÇA 2 [Ferramentas de Uso Obrigatório]	
Computador do Teletrabalhador	**Empresa**
Certificação Digital (PKI) Call-Back (somente para desktop operando em linha comutada)	Certificação Digital (PKI) Servidor de Acesso Remoto e Call-Back (somente para linhas comutadas) IDS Arquitetura de segurança complexa
NÍVEL DE SEGURANÇA 3 **[Ferramentas de Uso Opcional]**	
Computador do Teletrabalhador	**Empresa**
Criptografia de arquivos sensíveis em desktops* Token-Card Biometria Alarme residencial Sistema de Vigilância	Criptografia de arquivos sensíveis * Monitoração do Acesso Serviço de Diretórios LDAP Arquitetura de segurança mais complexa (* Uso obrigatório)

No nível de Segurança 2, as ferramentas relacionadas também são de uso obrigatório. Tratam-se de ferramentas de uso menos freqüente, com custo mais elevado e implementação mais complexa, como no caso do IDS e da PKI. Nesse nível, se a comunicação for por meio de linha comutada, deve ser empregado um servidor de acesso remoto com protocolo RADIUS ou TACACS para autenticação dos usuários. Opcionalmente, no caso dos teletrabalhadores com telefone fixo, também pode-se empregar um sistema de *Call-Back* para que, somente telefones previamente autorizados obtenham acesso.

No nível de segurança 3, a criptografia de arquivos sensíveis é obrigatória, sendo as demais ferramentas de uso opcional, empregadas, conforme o caso, para elevar ao máximo o nível de segurança das informações do sistema. Em *notebooks*, a criptografia de arquivos sensíveis é obrigatória em todos os níveis.

Como mostra a figura 5.4, a implementação do nível de segurança 1 pode não fornecer uma solução “ideal” em termos de segurança, mas envolve custos menores, sendo, portanto, mais acessível. A implementação dos níveis 2 e 3 para maximização da segurança implica um rápido e substancial aumento dos custos, exigindo um investimento consideravelmente maior pela organização.

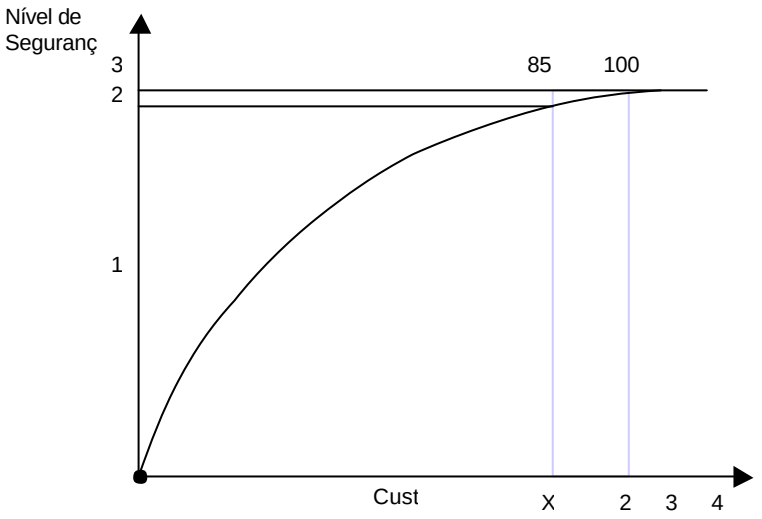

Figura 5.4: Investimentos/Custos dos Níveis de Segurança

Fonte: Adaptado de Internet Security Systems (2001). Disponível em: http://www.iss.net/securing_e-business/rms/ns_sn.php

A definição sobre qual nível de segurança será adotado pela empresa pode ser feita de forma subjetiva, simplesmente optando-se por um nível de segurança, sabidamente igual ou superior às necessidades do sistema existente.

O mais adequado, contudo, seria uma avaliação mais objetiva e criteriosa, fazendo-se necessário, para tanto, a realização de uma análise de riscos, conforme apresentado no item 5.3.3.

5.3.3 Análise e Avaliação de Riscos

A análise de riscos tem por objetivo determinar o nível de segurança do modelo necessário para cada empresa. Segundo Alberton (1996), a análise de riscos consiste no exame e detalhamento dos perigos identificados com o intuito de descobrir as causas e as possíveis conseqüências caso os acidentes aconteçam.

Dentre as técnicas de análise existentes, selecionou-se a APR (Análise Preliminar de Riscos) descrita por Alberton (1996) para ser aplicada ao modelo por possibilitar uma rápida definição do nível de segurança necessário. Trata-se de uma análise desenvolvida na área militar onde os riscos e sua categorização são definidos de acordo com a norma MIL-STD-882, conforme mostra o Quadro 5.3.

Quadro 5.3: Classificação do Acidente Quanto ao Fator Crítico
(Fonte: Ministry of Defense, 2001)

FATOR CRÍTICO				
	Tipo de Severidade			
Faixa de Probabilidade	Catastrófica	Crítica	Marginal	Desprezível
Freqüente	T4	T4	T3	T2
Provável	T4	T3	T3	T2
Ocasional	T3	T3	T2	T2
Remota	T3	T2	T2	T1
Improvável	T2	T2	T1	T1

Segundo esta classificação, os graus de severidade são:

(a) Desprezível: Não degrada o sistema ou seu funcionamento;

(b) Marginal: Degradação moderada com danos menores, compensáveis ou controláveis;

(c) Crítica: Degradação crítica com danos substanciais que colocam o sistema em risco, necessitando ações corretivas imediatas para a sua continuidade e

(d) Catastrófica: Séria degradação ou perda do sistema.

Com relação ao modelo de segurança proposto, pode-se situar o nível de segurança necessário da seguinte forma:

- **T1** e **T2** = Nível de segurança 1
- **T3** = Nível de segurança 2
- **T4** = Nível de segurança 3

A análise deve ser aplicada para cada tipo de ameaça, empregando-se o formulário mostrado no Quadro 5.4.

Quadro 5.4: Formulário para realizar a APR
(Fonte: Alberton, 1996)

IDENTIFICAÇÃO DO SISTEMA:				
IDENTIFICAÇÃO DO SUBSISTEMA:				
RISCO	CAUSAS	EFEITOS	CATEGORIA DO RISCO	MEDIDAS PREVENTIVAS OU CORRETIVAS

É importante salientar que o emprego da classificação proposta no quadro 5.3 tem por objetivo facilitar o processo de decisão sobre qual nível de segurança deve ser empregado e não deve engessar o modelo proposto. As necessidades e especificações do sistema, assim como a vontade da empresa, podem determinar o emprego de um outro nível de segurança cujo enquadramento não esteja em conformidade com o quadro 5.2.

Por outro lado, se a implementação do nível de segurança considerado mais adequado está além das possibilidades orçamentárias da empresa, pode-se optar pela implementação de um nível de segurança inferior ao ideal, assumindo-se os riscos desta decisão, ou ainda por não implementar o programa de teletrabalho. Da mesma forma, pode-se optar pela implementação de um nível de segurança superior ao necessário, buscando-se com essa medida a excelência da confidencialidade.

5.3.4 Controles de Segurança

Com base nas recomendações e controles genéricos para sistemas de teletrabalho estabelecidos no item 9.8 da norma ISO/DIS 17799 (Anexo A), criou-se um conjunto de quatorze controles que envolvem todos os aspectos do sistema, incluindo *hardware, software* e *peopleware*, descritos a seguir.

Esses controles devem ser empregados como base para implementação efetiva da segurança no sistema, podendo ser alterados conforme as necessidades específicas de cada organização, mas, de forma alguma, podem ser ignorados.

Os controles se aplicam a todos os níveis de segurança do modelo. Os controles 13 e 14, contudo, propõe a utilização de ferramentas de segurança que dependem do nível de segurança selecionado.

(1) **Recursos:** Deve-se especificar qual é a proveniência dos equipamentos básicos (computador, adaptador de rede e modem) e do canal de comunicação usados para o desempenho das atividades de teletrabalho: se serão fornecidos pela empresa ou se serão disponibilizados pelo teletrabalhador;

(2) **Inspeção:** Deve-se especificar quais inspeções devem ser realizadas pela equipe de segurança no sistema do teletrabalhador e com que freqüência, com objetivo de localizar e eliminar viroses, *trojans*[2], *sniffers*[3] , e outras ameaças semelhantes;

[2] Trojan: Programa invasor que afeta o sistema, comprometendo seu funcionamento normal.
[3] Sniffer: Programa capaz de monitorar a comunicação de dados no sistema, possibilitando o rastreamento de nomes e senhas de seus usuários.

(3) **Aplicativos:** Os aplicativos necessários às atividades do teletrabalhador, incluindo os aplicativos de segurança e comunicação, devem ser instalados pela equipe de segurança;

(4) **Acesso:** Deve ser especificado o período e os direitos de acesso, assim como a política de senhas para o acesso ao sistema pelo teletrabalhador;

(5) **Suporte:** O suporte ao teletrabalhador deve ser fornecido pela equipe de informática ou pela equipe de segurança, conforme o suporte necessário, seja referente a aplicações convencionais ou às aplicações de segurança, respectivamente;

(6) **Manutenção:** A manutenção no *hardware* do sistema deve ser efetuada, quando terceirizada, por empresa homologada pela equipe de segurança;

(7) **Cópia de Segurança:** Deve ser especificada a forma como serão criadas cópias *backup* das informações processadas pelo teletrabalhador para assegurar sua integridade;

(8) **Disponibilidade:** Procedimentos de contingência devem ser estabelecidos para o caso de indisponibilidade do sistema, seja devido a falhas no computador do teletrabalhador, no sistema da empresa ou no canal de comunicação;

(9) **Revogação:** Com a finalização do programa de teletrabalho, as senhas e direitos de acesso remoto do teletrabalhador devem ser imediatamente revogados. Os equipamentos, quando pertencentes à empresa, devem ser recolhidos e seus discos-rígidos devem ser formatados para impossibilitar a recuperação de informações confidenciais. Quando os equipamentos forem de propriedade do teletrabalhador, todos os aplicativos devem ser completamente removidos;

(10) **Auditoria:** Deve ser realizada auditoria periódica no sistema para monitorar tentativas de acesso não autorizadas por meio da conta do teletrabalhador assim como para verificar a conformidade do sistema quanto à sua eficácia em resistir a ameaças;

(11) **Política de Segurança:** Deve ser fornecido ao teletrabalhador o acesso à política de segurança da empresa. Após tomar conhecimento da mesma, o teletrabalhador deve preencher uma declaração afirmando conhecer e entender a política de segurança da empresa;

(12) **Treinamento:** O teletrabalhador deve ser orientado pela equipe de segurança quanto a suas responsabilidades e riscos referentes à segurança da informação inerentes a suas atividades.

(13) **Ocorrências:** O teletrabalhador deve reportar imediatamente à equipe de segurança, quaisquer ocorrências que possam estar relacionadas a riscos para a segurança da informação no sistema. Independente desses reportes, um relatório por escrito deve ser preenchido periodicamente pelo teletrabalhador, informando eventuais ocorrências no sistema relacionadas à segurança, desempenho e funcionalidade, com o objetivo de aperfeiçoar o sistema.

(14) **Segurança Física:** A segurança física do sistema deve ser garantida por meio de uma inspeção às instalações do sistema na residência do teletrabalhador onde devem ser observadas a adequação dos aspectos ergonométricos, elétricos e ambientais para a realização das atividades de teletrabalho de forma satisfatória. Conforme a análise de riscos e as relações de custo e benefícios envolvidas também podem ser usadas as seguintes ferramentas, conforme o nível de segurança selecionado:

- Alarmes contra incêndio;
- Alarmes contra roubos e
- Câmeras de vídeo para monitoração do ambiente.

(15) **Segurança Lógica:** A segurança lógica do sistema do teletrabalhador deve ser garantida por meio do emprego obrigatório das seguintes ferramentas necessárias à implementação do nível de Segurança 1:

- VPN;
- *Firewall* Pessoal ;
- Anti-vírus e
- Estabilizador de tensão ou *No-Break*.

Conforme a análise de riscos e as relações de custo e benefícios envolvidas também poderão ser empregadas as seguintes ferramentas, especificadas para os Níveis de Segurança 2 e 3:

- Certificação Digital (Banda Larga)
- Servidor RADIUS, TACACS e *Call-Back* (Linha Comutada)
- Certificação Digital;
- Criptografia de arquivos;
- *Token Card*;
- Servidor de Acesso Remoto e
- Biometria.

O emprego de controles adicionais envolvendo monitoração e controle de acesso para maximizar a segurança é possível. Entretanto, por envolver maior custo e complexidade operacional, estes devem se restringir a casos especiais onde o teletrabalhador tenha acesso a informações muito críticas, capazes de comprometer seriamente a imagem ou a própria sobrevivência da organização

5.3.5 Incorporação dos Controles à Política de Segurança

Os controles desse modelo devem ser incorporados à política de segurança da empresa, cuja função é direcionar os esforços da organização para assegurar suas informações.

A política de segurança, conforme apresentado anteriormente, deve ser do conhecimento do teletrabalhador. Esse aspecto, assim como o treinamento desses, para teletrabalhar de forma segura, é fundamental para o bom funcionamento do sistema.

5.3.6 Arquitetura de Segurança

A figura 5.5, apresentada a seguir, mostra o modelo de segurança proposto e seus componentes. Considerou-se o fato de que a comunicação entre o teletrabalhador e a empresa pode ser realizada por meio de uma linha comutada ou por banda larga, via Internet .

O modelo de segurança proposto exige a utilização de um par de *firewalls*, sendo um deles corporativo, instalado na sede da empresa, e outro pessoal,

instalado no computador do teletrabalhador. A necessidade do *firewall* pessoal está no fato do teletrabalhador ter de se conectar à Internet (uma canal inseguro) para obter o acesso à empresa.

A segurança da comunicação de dados é garantida pela utilização de uma conexão VPN (Virtual Private Network) através da qual os dados são criptografados antes de serem transmitidos. Na empresa fica instalado um servidor de túneis virtuais baseados em criptografia e, na residência do teletrabalhador, um *software* ou um dispositivo externo com facilidade de VPN.

No Nível de Segurança 2, em adição à VPN, se o canal de comunicação for uma linha comutada, deve ser empregado o *Call-Back*, por meio do qual o teletrabalhador inicia a conexão com o servidor da empresa que retorna a ligação telefônica para o número telefônico da residência do teletrabalhador. Se a conexão for por banda larga (cable modem, xDSL, ISDN ou outra) deve ser empregado em substituição ao *Call-Back* um sistema de certificação digital baseado em esquema de chaves públicas – PKI.

No nível de segurança 2, a arquitetura da rede da empresa deve ser também acrescida de um IDS para detecção de intrusos que consigam vencer as barreiras oferecidas pelo *firewall*.

A segurança lógica Interna é garantida por um anti-vírus presente na empresa e no computador do teletrabalhador.

Um serviço de auditoria no sistema da empresa possibilita o acompanhamento da conta e das atividades do teletrabalhador a qualquer momento.

O acesso remoto da equipe de segurança por meio da conexão segura possibilita a realização do suporte e de inspeções periódicas no sistema do teletrabalhador com um custo reduzido.

O emprego de um servidor de acesso remoto do tipo RADIUS ou TACACS, que ocorre quando se emprega o acesso via linha comutada pode, conforme o caso, dispensar o uso do *firewall* para proteção da comunicação.

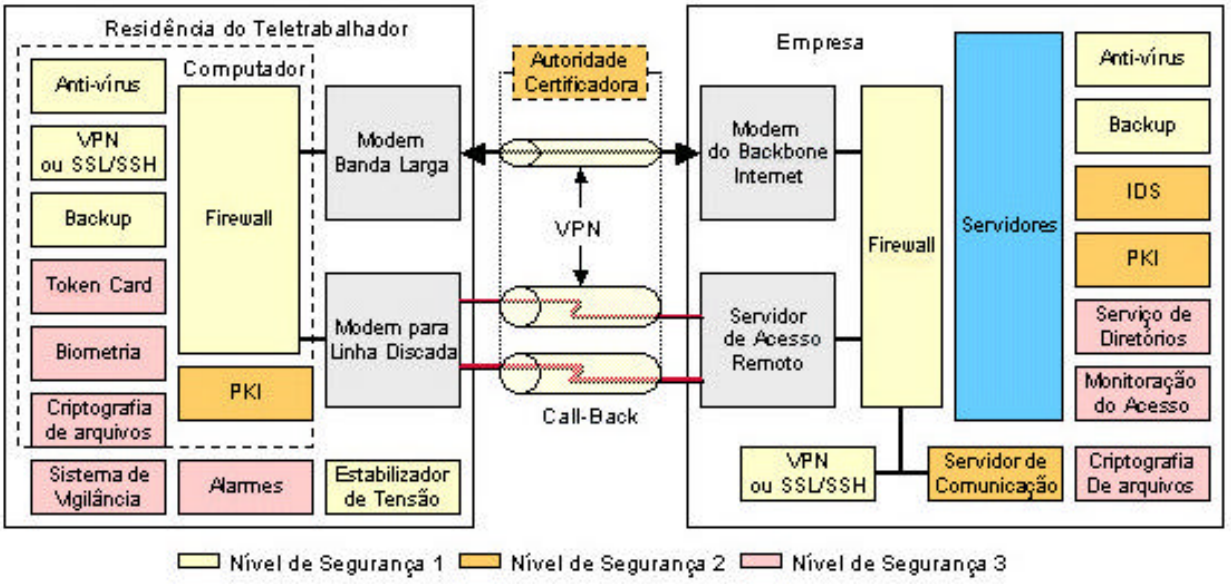

Figura 5.5: Arquitetura de Segurança do Modelo

5.3.7 Validação do Modelo de Segurança Delineado

É desejável a validação do sistema onde o modelo de segurança foi implementado, de forma a se determinar a efetividade das medidas e ferramentas empregadas e portanto o quão protegido ele está. Contudo essa é uma tarefa de difícil realização na medida em que não existe um consenso sobre quais métricas de segurança devem ser empregadas (NIELSEN, 2000).

Métricas são diferentes formas de aferição que podem ser usadas para demonstrar o estado atual da segurança e para estabelecer quais recursos são necessários para incrementá-la. Embora já existam métricas aplicáveis a produtos, tal como o *Comum Criteria*, trata-se de um assunto que ainda carece de maturação (NIELSEN, 2000).

Em virtude dessas restrições, McLean (1994) sugere o emprego de ferramentas baseadas em *software*, tal como o *Proteu* e o *Cobra*, que estabelecem seus próprios critérios para criar uma referência e medir o grau de conformidade de segurança da rede interna da empresa com relação a um padrão conhecido, por exemplo, a BS7799.

Tais ferramentas, contudo, não avaliam a totalidade da segurança. Testes envolvendo simulações de ataques teriam de ser realizados para se comprovar a

efetividade do sistema. Nesse sentido algumas empresas, tal como a Symantec (www.symantec.com) disponibilizam um serviço de avaliação, rápido e gratuito, via Internet, que possibilita avaliar o grau de proteção do sistema, seja no computador do teletrabalhador, seja no site da empresa. Outras empresas, especializadas em consultoria de segurança da informação, disponibilizam serviços semelhantes e mais completos. Por fim, a própria equipe de segurança da empresa pode realizar seus próprios testes de ataque visando a validação do sistema.

5.4 Sobre a Descrição Matemática do Modelo de Segurança

Kavanach (apud SALT, 2000), afirma ser impossível criar-se um modelo lógico matemático para atender diretamente às necessidades de enumerar as vulnerabilidades e respectivas contramedidas de um sistema. Para Kavanach, a teoria ainda não proporciona os subsídios necessários para áreas específicas quanto à implementação de segurança que depende de habilidades e experiências das pessoas responsáveis pela segurança.

De forma complementar, Denning (1999) argumenta que, embora a descrição matemática rigorosa de um modelo de segurança seja possível, ela seria muito cara e demorada, em grande parte devido ao fato de muitos sistemas comerciais não serem baseados em modelos matemáticos.

Em virtude dessas restrições, optou-se por não se descrever matematicamente o modelo proposto, o que determinaria, dentre outros aspectos, na especificação detalhada de marcas e modelos das ferramentas de segurança, o que implicaria em um engessamento do mesmo e a inviabilização de sua adoção por um grande número de organizações.

5.5 Limitações do Modelo de Segurança Delineado

Segundo Denning (1999), todos os modelos de segurança têm seus limites teóricos e práticos. Nem sempre é possível satisfazer a todos os requisitos de segurança desejados. De acordo com o referido autor, o emprego de um modelo de

segurança não implica em segurança total pois constantemente novas técnicas são criadas para fazer alterações indevida (*hacking*) de sistemas e produtos.

O emprego dos controles, baseados na ISO/DIS 17799, são uma forma efetiva de se criar uma política de segurança eficaz, contudo, conforme ressalta McLean (1994), o emprego de controles não é o suficiente para assegurar as informações. Para McLean, a formação de uma cultura de segurança da informação na empresa é uma peça de vital importância nesse esquema. A formação dessa cultura, seja por meio de treinamento, seja por outros meios de difusão, não pode ser negligenciada e dificilmente pode ser equacionada de forma matemática.

Levando-se em consideração estes aspectos, os fatores limitadores do modelo proposto são:

(a) Dependência do emprego de ferramentas cujo grau de eficiência pode variar muito, conforme sua implementação interna ou configuração durante a instalação e
(b) O grande número de variáveis envolvidas no sistema.

5.6 Validação do Modelo em uma Organização Concreta

Para validar o modelo de segurança, foi proposta sua implementação em uma organização pública vinculada ao Poder Executivo Federal, localizada em Brasília, DF.

A escolha desta organização ocorreu devido ao fato de a mesma estar implantando, no segundo semestre de 2001, um sistema com objetivo de possibilitar o teletrabalho a alguns de seus funcionários, inicialmente num total de quatro indivíduos, pertencentes ao quadro de executivos da empresa (nível gerencial).

Uma descrição do modelo foi entregue aos membros da equipe de informática da empresa, também responsáveis pela manutenção da segurança da informação por meio de ferramentas já implementadas.

Um formulário APR (Quadro 5.4 – Pg. 99) foi fornecido pelo pesquisador ao administrador da rede da empresa para que este realizasse uma análise de riscos envolvendo a segurança das informações da empresa, disponibilizadas em seu sistema de TI, que deveria ser acessado remotamente pelos teletrabalhadores. Essa

análise estabeleceu que, dentre o universo de possíveis ameaças para o programa de teletrabalho, as mais relevantes para essa organização, no momento, e que deveriam ser consideradas seriam:

1º Lugar: Invasão de rede interna por viroses de computador;
2º Lugar: Ataques externos, via Internet, de *Hackers* e
3º Lugar: Roubo dos computadores dos teletrabalhadores (notebooks).

O Quadro 5.5, apresentado a seguir, mostra a ficha APR, descrita anteriormente, tal como foi preenchida pelo administrador da rede.

Quadro 5.5: Formulário APR da Organização para o Programa de Teletrabalho

RISCO	CAUSAS	EFEITOS	CATEGORIA DO RISCO	MEDIDAS PREVENTIVAS OU CORRETIVAS
Vírus	E-mail contaminado, Falha no Anti-vírus	Destruição de arquivos, corrupção de programas	T2	Atualização automática do anti-vírus Backup Periódico
Ataque externo	Falha na configuração ou defeito no firewall	Corrupção da Intranet da empresa, acesso a dados sigilosos	T2	Atualização e testes periódicos do firewall Backup Periódico
Roubo do computador do teletrabalhador	Descuido do teletrabalhador	Comprometimento da segurança de acesso	T2	Uso de criptografia em informações sigilosas existentes nos computadores

Com base na classificação dos acidentes quanto ao fator crítico (quadro 5.3 – Pg. 98), os riscos foram todos enquadrados no nível T2, que, conforme o modelo de segurança, indica a necessidade de implementação do nível 1 de Segurança.

A equipe de informática da organização concluiu que, em face dos riscos existentes, o nível de segurança 1 seria satisfatório para atender às necessidades

do sistema, uma vez que, à exceção da VPN, as demais ferramentas de segurança previstas já estavam em uso na empresa, e mesmo para a VPN, não haveria custo adicional para sua implementação já que ela estaria disponível como uma facilidade extra do *firewall* em uso na empresa.

Com relação aos computadores dos teletrabalhadores, a equipe de informática decidiu que todos empregariam *notebooks*, não só pela necessidade de acessarem a empresa quando estivessem viajando, como também para facilitar o controle do conteúdo dos mesmos (programas instalados) pela equipe de informática.

Foi decidido que esses computadores usados pelos teletrabalhadores empregariam as seguintes ferramentas previstas no modelo:

- **Firewall Pessoal:** Zone Alarm 2.6 (disponível em: www.zonelabs.com);
- **Anti-vírus:** McAfee Anti-vírus (disponível em: www.mcafee.com);
- **VPN:** Cliente VPN do *firewall* corporativo
- **Backup:** Sistema de *backup* do servidor de rede e
- **Criptografia:** PGP[4] versão 2.6.2

Um problema surgido durante a implementação foi a indisponibilidade do módulo VPN para o *firewall* em uso na empresa. Embora o fabricante prometesse liberar essa facilidade para o próximo *release* do produto, optou-se por empregar um sistema de criptografia de comunicação disponibilizado no mesmo *firewall*, de forma a não atrasar os testes do sistema, cujos resultados em termos de proteção seriam próximos aos da VPN.

Ao se aplicar os controles de segurança, descritos no item 5.3.4, a equipe de informática alegou que seria muito difícil convencer os teletrabalhadores, em função de sua posição hierárquica e de outros problemas administrativos internos, sobre a necessidade de se implementar aqueles controles, como estavam especificados.

Optou-se, portanto, por alterar a redação dos controles 2 e 12, onde originalmente estavam previstos os períodos de inspeção e de apresentação de relatórios, respectivamente, deixando esses períodos em aberto para que a empresa os estabelecesse, conforme suas possibilidades. Essas correções, assim como

outras, de menor monta, relacionadas à questão da compreensão do texto, foram assim incorporadas aos controles descritos no item 5.3.4.

Com relação ao item 13, (Segurança física) fez-se compreender que a inspeção ao local de trabalho do teletrabalhador (sua residência) era fundamental para assegurar o sistema.

Ao aplicar os controles de segurança, foram definidas as seguintes características pela equipe de informática para o sistema de teletrabalho:

- **Equipamento:** O computador, *do tipo notebook*, com todos os acessórios necessários às atividades de teletrabalho, será fornecido pela empresa;
- **Inspeções:** Serão realizadas pela equipe de informática no computador do teletrabalhador: uma inspeção inicial, antes da entrega do computador ao mesmo, uma inspeção trimestral para avaliação das condições de segurança do sistema; e inspeções eventuais, após a realização de cada manutenção do computador;
- **Aplicativos:** A instalação de aplicativos e atualizações no computador serão feitos exclusivamente pela equipe de informática;
- **Acesso:** O acesso do teletrabalhador poderá ser feito 7 dias por semana, 24 horas por dia com direitos de acesso menores dos que os da rede Interna e com senha para acesso remoto independente da senha para acesso à rede, obedecendo aos mesmos parâmetros de comprimento, duração e bloqueio desta última;
- **Suporte:** O suporte ao teletrabalhador será fornecido pela equipe de segurança por meio de acesso remoto ou, de forma presencial, quando o primeiro não for possível ou suficiente;
- **Manutenção:** A manutenção do computador, quando externa, deverá ser realizada por uma assistência autorizada pelo fabricante do computador;
- **Backup:** Para sofrerem *backup*, as informações produzidas ou processadas pelo teletrabalhador devem ser enviadas para um servidor previamente designado na rede que seja submetido ao processo de *backup* dentro da rotina normal da rede e
- **Revogação:** Com o encerramento das atividades do teletrabalhador, as senhas e direitos de acesso remoto devem ser revogados imediatamente; o computador

[4] Pretty Good Privacy – Tradicional programa empregado para proteger dados através de criptografia

deve ser recolhido e seu disco-rígido deve ser completamente formatado para evitar qualquer tipo de recuperação de informações confidenciais.

A implementação das ferramentas, sua configuração e os testes de acesso por parte dos teletrabalhadores transcorreram, sem maiores incidentes, ao cabo de quatro dias, em novembro de 2001.

Os testes de acesso envolveram dois computadores *notebooks* dos teletrabalhadores, inicialmente instalados no departamento de informática da empresa e, posteriormente, na residência de dois teletrabalhadores previamente selecionados para executar os testes.

Os sistemas acessados remotamente incluíram a *Intranet* da empresa, transferência de arquivos MS Word e MS Excel, envio de correio eletrônico (interno) e acesso ao banco de dados corporativo.

Os acessos foram feitos por meio de linhas telefônicas comutadas convencionais instalados nos *notebooks*, verificando-se que a velocidade de operação, à exceção do acesso ao banco de dados, demonstrou ser satisfatória.

Para se validar a segurança, foi empregada a facilidade de testes do site da empresa Symantec, disponível na Internet (www.symantec.com) apenas para os computadores dos teletrabalhadores, pois o sistema da empresa já havia sido testado recentemente por meio de simulações de ataque pela própria equipe de informática. Essa mesma equipe agendará, oportunamente, testes mais detalhados para aferir a confiabilidade dos computadores dos teletrabalhadores.

Com a conclusão desses testes, a equipe de informática encaminhou um relatório dando ciência à diretoria da empresa dos testes realizados e dos controles de segurança que deverão ser empregados para garantir a segurança do sistema.

5.7 Considerações Finais

O modelo de segurança proposto restringe-se a proporcionar um grau adequado de segurança. Vale assinalar que a implementação de um programa eficiente de teletrabalho requer também o desenvolvimento de um plano de contingência para assegurar a disponibilidade e integridade das informações.

O objetivo do modelo foi o de proporcionar, de forma rápida e eficiente, o estabelecimento de um programa de teletrabalho que contemple a segurança das informações. Esse objetivo foi alcançado durante seu processo de validação. Novos casos de implantação do modelo a serem realizados no futuro poderão contribuir para seu aperfeiçoamento.

A implementação do modelo na prática demonstrou as dificuldades advindas de uma metodologia de implantação *bottom-up* (de baixo para cima) da política de segurança. Tal como descrito do Capítulo 2, as iniciativas que partem da base da pirâmide hierárquica da empresa, representada nesse caso pela equipe de informática da mesma, são mais difíceis de serem aceitas do que quando a iniciativa parte do topo da hierarquia (metodologia top-down).

É importante ressaltar que, para se assegurar a eficácia do modelo, são fundamentais, após sua implementação, o treinamento do teletrabalhador quanto às medidas de segurança e a realização de auditorias periódicas em busca de falhas, de forma a possibilitar a contínua revisão, atualização e aperfeiçoamento do modelo implantado.

Fica, por fim, lançada a proposta, para futuras pesquisas, de desenvolvimento de um sistema de métricas de segurança que confira maior precisão ao modelo com relação à aferição da segurança do sistema.

6 CONCLUSÃO E FUTUROS DESENVOLVIMENTOS

6.1 Conclusão

Conforme foi apresentado ao longo desse trabalho de pesquisa, o teletrabalho é uma proposta de atividade produtiva que se iniciou no começo dos anos 70, com experiências precursoras que remontam ao século XIX.

Nos dias atuais, em função do tempo despendido com deslocamentos no trânsito e por questões ecológicas envolvendo a poluição do ambiente, o teletrabalho vem ganhando espaço, paulatinamente, nas organizações. Esse aspecto é verdadeiro especialmente nas empresas cujas atividades são relacionadas à área da informação, de tal sorte que, na Europa, já se contabilizam 9 milhões e nos Estados Unidos da América, 20 milhões de teletrabalhadores.

Na medida em que as telecomunicações e o acesso à computação se massificaram, ao longo das últimas décadas, aumentaram muito as ameaças à segurança da informação, pois tornou-se possível o acesso (devido ou não) de milhões de pessoas aos sistemas de TI das empresas.

Ao mesmo tempo em que novas ameaças foram surgindo e crescendo em volume, ferramentas, técnicas de análise e controles de segurança também foram sendo criados para atuar como contramedidas para essas ameaças.

Inicialmente o acesso aos sistemas de TI das empresas era feito sem quaisquer medidas de segurança, as quais foram sendo criadas ao longo do tempo, na medida em que os riscos de violação foram aumentando.

A norma ISO/DIS 17799, homologada em 2000, após 5 anos de desenvolvimento, é o mais recente esforço no sentido de levar uma solução de gerenciamento da segurança das informações ao alcance da maioria das empresas.

Efetivamente, essa norma, de uso público, possibilita a criação de controles que podem ser empregados para a gestão da maioria dos aspectos da segurança da informação, tal como os que foram empregados nesse trabalho, podendo ser incorporados diretamente na política de segurança das empresas.

Para responder à pergunta de pesquisa “Como gerenciar a segurança da informação em sistemas de teletrabalho?” apresentada no Capítulo 1, foram definidos, como objetivos preliminares específicos, uma apresentação das relações

entre o teletrabalho e a segurança da informação e uma análise sobre como as organizações brasileiras que se utilizam do teletrabalho estão tratando essa questão.

Para atingir esses objetivos específicos, o presente trabalho produziu uma pesquisa bibliográfica apresentada no Capítulo 2 e uma pesquisa descritiva, apresentada nos Capítulos 3 e 4.

A relevância da pesquisa bibliográfica está no fato de o tema “teletrabalho x segurança da informação” ter sido, até então, pouco abordado pela comunidade científica: não existem livros sobre o tema; são poucos os artigos produzidos e a maior parte das referências existentes são caracterizadas pela superficialidade teórico-prática. Nesse sentido, esse trabalho aglutinou a maior parte das informações relevantes, proporcionando uma visão detalhada sobre essa questão.

A pesquisa teórico-empírica cujos resultados foram expostos no Capítulo 4, demonstrou que muitas organizações já estão atentas para a questão da segurança das informações no que diz respeito ao teletrabalho. Contudo, mesmo essas ainda têm pontos em suas políticas de segurança para serem aperfeiçoados, uma vez que poucas organizações tomaram conhecimento de recentes aperfeiçoamentos nesse campo, tal como a criação da norma ISO/DIS 17799. A pesquisa também demonstrou que as empresas empregam principalmente as ferramentas de segurança referendadas pelo mercado e de uso já disseminado.

Para responder à pergunta de pesquisa e alcançar o objetivo específico de propor uma metodologia para gerenciamento da segurança das informações para empresas que empregam o teletrabalho, foi criado um modelo de segurança para teletrabalho, apresentado no Capítulo 5. Esse modelo foi baseado no emprego das ferramentas atualmente em uso que possibilitam assegurar a integridade, confidencialidade e disponibilidade das informações nas empresas.

Partindo-se de um contexto de “acesso remoto à rede”, onde a segurança das informações baseava-se em uma única ferramenta de controle de acesso, em geral proprietária, essa dissertação propôs um modelo de segurança não mais voltado para o “acesso remoto” (que na realidade é uma atividade meio), mas sim para a atividade fim, que é a “realização do teletrabalho”.

Em outras palavras, na antiga abordagem, o foco estava no uso propriamente dito de ferramentas de segurança, ao passo que o modelo proposto propõe uma

abordagem global onde a componente *peopleware*, ou seja, o teletrabalhador, é tão importante quanto os tradicionais componentes *hardware* e *software*.

Além disso, a metodologia proposta por meio do modelo de segurança tem por objetivo atender a todos os interessados em teletrabalho e não apenas a profissionais e especialistas em informática, como era o caso da antiga abordagem. Nesse sentido o modelo proposto possibilita estabelecer o nível de segurança que a organização deseja, as ferramentas e os controles necessários de forma rápida e eficiente, dispensando o concurso de consultorias em segurança da informação ou maiores prospecções por parte da empresa.

A aplicação do modelo na prática revelou que o emprego dos controles é muito influenciado pela política administrativa da empresa, necessitando adequações conforme cada caso. Essa, contudo, é a forma de operacionalização prevista pela norma ISO/DIS 17799, com base na qual os controles de segurança foram estabelecidos.

6.2 Sugestões para Trabalhos Futuros

Como proposta para futuros trabalhos e pesquisas sugere-se o desenvolvimento de um sistema de métricas de segurança que possa ser aplicado ao modelo, sem contudo, onerar significativamente o custo de sua implementação. Sugere-se também uma descrição matemática do mesmo e, por fim, a realização de novos estudos de caso que concorram para seu aperfeiçoamento.

O modelo proposto está vinculado a ferramentas de segurança que, certamente, ao longo do tempo, sofrerão modificações e aperfeiçoamentos, podendo algumas serem descontinuadas ou sofrerem alterações de tal magnitude que impliquem em mudanças de algumas das características do modelo.

Por outro lado, os controles propostos para o modelo de segurança, baseados na ISO/DIS 17799, podem exigir mudanças nos procedimentos administrativos e operacionais das empresas em que foram aplicados.

Assim, muitas empresas que já mantêm programas de teletrabalho precisarão apenas ajustar suas políticas de segurança para incorporar os controles propostos pelo modelo, uma vez que já empregam algumas das ferramentas de segurança

previstas. Se, à primeira vista, esse processo de incorporação possa parecer fácil, devido a não necessidade de novos investimentos, alerta-se que a alteração dos procedimentos administrativos da empresa, ou da rotina de seus funcionários, pode se configurar na parte mais desafiadora do processo. Por outro lado, algumas organizações talvez tenham que rever completamente seus sistemas para se adequarem às especificações do modelo proposto.

Acredita-se que os principais beneficiários desse trabalho serão as organizações que ainda não aderiram ao teletrabalho e que virão a fazê-lo futuramente, na medida em que terão um modelo de segurança válido para sua utilização.

Por fim, com a conclusão desse trabalho, prosseguem os esforços de pesquisa anteriormente mencionados e o objetivo de divulgar para as organizações e o público, em geral, os resultados da pesquisa realizada e o modelo de segurança proposto.

Pretende-se, com isso, dar uma aplicação prática e justa a esse trabalho, contribuindo com os esforços de se expandir as possibilidades de teletrabalho, gerando benefícios diretos para essas organizações e para a sociedade.

7 REFERÊNCIAS

ALBERTON, A. **Uma metodologia para auxiliar no gerenciamento de riscos e na seleção de alternativas de investimentos em segurança**. 100f. Dissertação (Mestrado em Engenharia de Produção) – Programa de Pós-Graduação em Engenharia de Produção – UFSC, Florianópolis. 1996. Disponível em: <http:// http://www.eps.ufsc.br/disserta96/anete/index/indx_ane.htm>. Acesso em: 29 jul. 2001.

ANDERSON, R. **Telecommuting trend means security concerns**. LocalBussiness.com. 2000. 2p. Disponível em: <http:// http://www.localbussiness.com/story/print/0,1197,nocit_209401,00.html>. Acesso em: 26 jun. 2001.

ANDRADE, E.L. **Introdução a pesquisa operacional – métodos modernos de análise de decisão**. 2ª Ed. Rio de Janeiro: Livros Técnicos e Científicos Editora. 2000.

ANDREASSI, T. **Virtualização das organizações: o caso do teletrabalho em uma consultoria**. Revista de Administração, São Paulo, v 32, n 4, p.77-83. 1997.

BALIEIRO, S. **Broadband para quê?** São Paulo: Exame Informática, ano 16, n 186, p 90. set. 2001.

BEHAMOU, E. et al. **Smart valley telecommuting guide**. Santa Clara, 1998. Disponível em: <http://www.svi.org/telecommuting>. Acesso em: 2 maio 2001.

BELL, M; ROSS, C. **Workplace transformation: a business imperative, strategic analysis report**. Base de Dados Gartner. 2000. Versão 2.1.

BERRY, S. **Telework today**. Computing & Control Engeenering Journal. 7 p.1996.

BENSON, P. **EMS-global security model**. 2001. 9p. Disponível em: <http://www.ems-global.com/index.htm>. Acesso em 29 maio 2001.

BRYDEN, J. **Standarts governance – good and bad**. 2001. 8p. Disponível em: <http://www.firetrench.net/riskcont.html>. Acesso em 27 maio 2001.

CARUSO, C.A.A.; STEFFEN, F.D. **Segurança em Informática e de Informações**. São Paulo: Ed. Senac. 1999.

CASCIO, W. **Managing a virtual workplace**. The Academy of Management Executive, Ada. 11 p. 2000.

CASTELS, M. **A Sociedade em rede**. 4ª Ed. São Paulo: Ed. Paz e Terra. 2000.

CARTWRIGHT, W. **Managing security in a mobile environment**. 2001. Sans Institute. 3p. Disponível em: <http://www.sans.org/infosecfaq/travel/managing_sec.htm>. Acesso em 28 maio 2001.

CHIAVENATO, I. **Teoria geral da administração**. 3ª Ed. São Paulo: Ed. McGraw-Hill. 1987.

CHEN, A. **Companies strike back at mobile hacks**. eWEEK. 2000. Disponível em: <http:// http://news.zdnet.co.uk/story/0,,s2083059,00.html>. Acesso em: 24 jun.2001.

CISCO NETWORKS. **How to get it right the first time**. San Jose. 1999. 6 p. Disponível em: <http://www.cisco.com/warp/public/784/packet/july99/25.html>. Acesso em: 27 abr. 2001.

CISCO NETWORKS. **Cisco telecommuting & remote user solutions**. San Jose. 6 p. 1999. Disponível em: <http:// ww.cisco.com/warp/public/cc/so/neso/axso/telecom/telec_ds.htm>. Acesso em: 27 abr. 2001.

COBB, S. **The mother of all security standarts?** Spectria Infosec Article. 3p. 2001. Disponível em: <http://www.infosec.spectria.com/articles/art-bs7799.htm>. Acesso em 27 maio 2001.

CONNOR, D. **Net managers find (remote) backing up hard to do.** Framingham: Network World. 2000.

COUTANCHE, B. **BS7799**. 2001. Disponível em: <http://www.coutanche.com/html/body_bs7799.html>. Acesso em: 22 maio 2001.

CSI. **2001 CSI/FBI computer crime and security survey**. San Francisco: Computer Security Issues and Trends. v 7, n 1, 18p. 2001.

DALAL, S. **Telecommuting security concerns**. Stillwater, Oklahoma: Oklahoma State University. 11p. 1999. Disponível em: <http://www.mstm.okstate.edu/faculty/weiser/fall99/tecom5350/papers/index.htm>. Acesso em: 6 jun. 2001.

DAVIES, R. **Internet conference on telecommuting**. Career Developement International, Australia, Institute of Team Management Studies, Milton, Queensland Australia and Editor. 1996.

DENNING, D.E. **The limits of formal security models**. National Computer Systems Security Award Acceptance Speech. 4p. 1999. Disponível em: <http://www.cs.georgetown.edu/~denning/infosec/award.html>. Acesso em: 18 jun. 2001.

DEIGHTON, N. et al. **The nest gerenation of mobile networks poses a $100 billion challenge for europe**. Strategics Analysis Report, Gartner Group. 2000.

DRUCKER, P. **Desafios gerenciais para o século XXI**. 1ª Ed. São Paulo: Ed. Pioneira. 1999.

DUNNING, A.E. **Telecommuting policy: Implementation and efficacy**. Georgia Institute of Technology City Planning. 1997.

ETO. **Telework (telecommuting): the benefits - and some issues**. Londres. Disponível em: <http://www.eto.org.uk/faq/faq03.htm>. Acesso em: 20 maio 2001.

FAGAN, P. **Some solutions to possibile e-commerce fraud**. Ukceb Journal. 8p. 2000. Disponível em: <http://wwwukceb.org/pub/newslet/aut2000/p12m0.html>. Acesso em: 27 maio 2001.

FERREIRA, A.B.H. **Novo dicionário da língua portuguesa**. 2ª Ed. São Paulo: Ed. Nova Fronteira. 1995.

FRASER, B. **RFC 2196, site security sandbook**. Reston: IETF. 1997. Disponível em: <http:// www.ietf.org>. Acesso em: 5 jan. 2001.

GAO. **Information security management – learning from leading organizations**. 62p. United States General Accounting Office. 1998.

Gil. A.C. **Como elaborar projetos de pesquisa**. 3ª Ed. São Paulo: Ed. Atlas. 1996.

GIRARD, J; ANDERSON, C. **Telecommuting with employee-owned home computers can cause problems**. Gartner Group. 15p. 1999.

GONÇALVES, M. **Firewalls – guia completo**. 1ª Ed. 2000. Ed. Ciência Moderna. Rio de Janeiro.

GOSLAR, M. **Telecommuting + telecomputing = telechallenging!** IT Management. 4p. Disponível em: <http://www.itmanagement.earthweb.com/secu/print/0,11953_621201,00.html>. Acesso em: 3 jun. 2001.

_____. **The new e-security frontier**. Information week. 2001. Disponível em: <http://www.iweek.com>. Acesso em: 12 ago. 2001.

GUTTMAN, E et al. **RFC2504 – user´s security handbook**. IETF. 1999. Disponível em: <http://www.ieft.org>. Acesso em: 8 ago. 2001.

HEFFERAN, C. **BS7799 – information security management**. 4p. 2000. Disponível em: <http://www.istc.org.uk/bs7799.htm>. Acesso em: 26 maio 2001.

HIRSCH, J.L. **Telecommuting: security policies and procedures for the "work-from-anywhere" workforce**. Sans Institute. 4p. 2000. Disponível em: <http://www.sans.ogr.infoseqfaq/homeoffice/telecom.htm>. Acesso em28 maio 2001.

HUBERMAN, L. **História da riqueza do homem.** 15ª Ed. Rio de Janeiro: Ed. Zahar Editores. 1979.

INTERNET SECURITY SYSTEMS. **Net secure and secure steps – a comprehensive risk management solution**. 4p. 2001. Disponível em: <http://www.iss.net/securing_e-business/rms/ns_sn.php>. Acesso em: 8 ago. 2001.

ISO17799. **International standart iso/iec17799 – information technology – code of practice for information security management**. International Standartization Organization. Genebra. 2000.

ITAC. **Telework America national telework survey for the International Telework**. Association & Consiul. Washington. Disponível em: <http://www.telecommute.org/twa/twa%5Fresearch%5Fexec%5Fsummary.doc>. Acesso em: 20 maio 2001.

JAMIL, G.L. **Repensando a ti na empresa moderna – atualizando a gestão com a tecnologia da informação**. 1ª Ed. Rio de Janeiro, Ed. Axel Books. 2001.

KAVANAGH, K. **The role of mathematical logic in designing secure systems**. 2001. SANS Institute. Disponível em: <http://www.sans.org/infosecfaq/audit/math_logic.htm>. Acesso em: 18 jun. 2001.

KUGELMASS, J. **Teletrabalho: novas oportunidades para o trabalho flexível**. 1ª Ed. São Paulo: Ed. Atlas. 1996.

KUNDUN, K. **Telecommuting: work is virtually something you do, not somewhere you go.** Washington. 1999. Disponivel em: <http://www.epf.org/etrend/tr991123.htm>. Acesso em: 20 maio 2000.

KURLAND, N.B.; BAYLEY, D.E**. Telework: the advantages an challenges of working here, there, anywhere, and anytime**. Organizational Dynamics. 1999.

KWOK, L.; LONGLEY, D. **Information security management and modeling**. 1999. 15p. Information Security & Computer Security. v 7, n 1. Disponível em: <http://www.emerald.com>. Acesso em: 29 maio 2001.

LAINHART, J.W. **COBIT – an update and look into the future**. ISACA. 6 p. 2001. Disponível em: <http://www.isaca.org/ct_art2.htm>. Acesso em: 01 abr. 2001.

LAUDON, K.C.; LAUDON, J.P. **Sistemas de informação**. 4ª Ed. Rio de Janeiro, Ed. Livros Técnicos e Científicos. 1999.

LEONHARD, W., **The underground guide to telecommuting**. 1ª Ed. Boston: Addison-Wesley Massachusetts Publishing Company. 1995.

LÈVY, P. **O que é o virtual?** 1ª Ed. São Paulo: Ed. 34. 1996.

MAGALHÃES, A.D. et AL, **Auditoria das organizações - metodologias alternativas ao planejamento e à operacionalização do métodos e das técnicas**. 1ª Ed. São Paulo: Ed. Atlas. 2001.

MANN, S. et Al, **An exploratin of the emotional impact of tele-working via computer-mediated communication**. Journal of managerial Psychology, v.15, n 7. 2000.

MARCONI, M.A.; LAKATOS, E.M> **Metodologia do trabalho científico**. 5ª Ed. São Paulo: Ed. Atlas. 2001.

McADAMS, A. **The evolution of the U.S. infrastructure over the next decade – broad bandwidth through dsl**. Cornel University. TTG-4. 13p. 1999. Disponível em: <http:// http://www.ieeeusa.org/committees/CCIP/workshop/TTG4.pdf>. Acesso em 26 jun. 2001.

McLEAN, J. **Security models**. 19p. 1994. Disponível em: <http://chacs.nrl.navy.mil/publications/chacs/1994/1994mclean-ency.pdf>. Acesso em: 20 jun. 2001.

MELLO, A. **Teletrabalho – telework**. 1ª Ed. Rio de Janeiro: Ed. Qualitmark. 1999.

MERIDIAN TECHNOLOGY CORPORATION. **Reinventing the workplace**. 1997. Disponível em: <http://www.meridian.com>. Acesso em: 15 maio 2001.

MICHAELIS, **Dicionário prático inglês-poruguês-português-inglês**. 24ª Ed. São Paulo: Ed. Melhoramentos. 1987.

MÓDULO. **Homologada a norma ISO17799**. Brasília. Módulo Notícias. 2001. Disponível em: <http://modulo.com.br/notícias>. Acesso em: 20 jan. 2001.

MOUSTAFA. N. **Worry-less wireless**. Overland Park: Wireless Review. v 17, n 22, 3p. 2000.

MUTSAERS, E.J. et al. **The evolution of information technology**. Information Management & Computer Security, v 6, n 3.1998.

NIELSEN, F. **Approaches to security metrics**. 15p. National Institute of Standarts and Technology. 2000.

NILLES, J.M. **What does telework really to do us?** World Transport Policy & Practice, v 2 n 1/2 . 1996.

_____. **Fazendo do teletrabalho uma realidade**. 1ª Ed. São Paulo: Ed. Futura. 1997.

OLIVEIRA, T.M.V. **Amostragem não probabilística: adequação de situações para uso e limitações de amostras por conveniência, julgamento e quotas**. Administração On-line, São Paulo, v 2, n 3, jul. 2001. Disponível em: <http:// http://www.fecap.br/adm_online/art23/tania2.htm>. Acesso em: 15 fev. 2002.

OPPENHEIMER, P. **Projeto de redes top-down – um enfoque de análise de sistemas para o projeto de redes empresariais**. 1ª Ed. Rio de Janeiro: Ed. Campus. 1999.

PASQUALI, L. **Intrumentos psicológicos: manual prático de elaboração**. 1ª Ed. Brasília: Laboratório de Pesquisa em Avaliação e Medida - IBAP. 1999.

PINTO, N.F.C.M. **Metodologia do trabalho científico**. Belo Horizonte: Instituto de Ciências Econômicas e Sociais, Curso de Administração - PUC-MG. 136 p. 2001.

PLISKIN, N. **The telecommuting paradox**. Boston, Harvard Business School, Massachussets, USA. 1997.

PURCELL, J. **Securing information on laptops computers.** Sans Institute. 3p. 2000. Disponível em: <http://www.sans.org/infoseqfaq/travel/sec_info.htm>. Acesso em: 28 maio 2001.

REID, F. **Securing the mobile businessman.** 2000. Sans Institute. 3p. Disponível em: <http://www.sans.org/infosecfaq/travel/mobile.htm>.
Acesso em 28 maio 2001.

REYMERS, K. **Telecommuting: on the re-integration of work and family**. Buffalo: Department of Sociology - Red Feather Journal of Sociology. 11p. 1998.

ROBERTI, M. **Building an enterprise security architecture**. 2001. 6p. Sans Institute. Disponível em: <http://www.sans.org/infosecfaq/policy/sec_arch.htm>. Acesso em 28 maio 2001.

ROBIETTE, A. **BS7799 and other security frameworks**. Disponível em: <http://www.jisc.ac.uk/pub01/security_policy.html>. Acesso em 28 maio 2001. 4p.

ROGNES, J. **Paradoxes and some unexpected consequences in telecommuting**. Estocolmo: Stockholm Scholl of Economics, 9 p. 1996.

SABBATINI, R.M.E. **Realidade virtual e medicina.** Campinas: Revista Infomédica, 1(1): 5-11, 1993. Disponível em:<http:// http://www.epub.org.br/informed/virtual.htm>. Acesso em: 20 maio 2001.

SANTILLO, L. **Common criteria or ISO17799.** 2001. 6p. Sans Institute. Disponível em: <http://www.sans.org/infoseqfaq/standarts/iso17799.htm>. Acesso em: 28 maio 2001.

SCAGLIA, A. **Tem de latir e morder**. São Paulo: Information Week, ano 3, n 53, pg 42, set. 2001.

SCHILL, A.; BRAUN, I. **Experiences with regional teleworking support for small and medium-sized enterprises**. Dresden: Chair for Computers Networks, Dresden University of Technology, Germany. 1999.

SCHNEIER, B. **Segurança.com – segredos e mentiras sobre a proteção na vida digital**. 1ª Ed. São Paulo: Ed. Campus. 2001.

SIEMENS. **Siemens at Cebit´98: telecommunications solutions for all areas of application**. Disponível em:
<http://www.icn.siemens.com/icn/news/1998/98021101.html>.
Acesso em: 15 de maio 2001.

SOARES, A. **Teletrabalho e comunicação em grandes cpds.** São Paulo: Revista de Administração de Empresas, v 35, n 2, pg 64-77. 1995.

SOLMS, R.V. **Information security management (2): the code of practice for information security management (BS7799)**. Information Security & Computer Security v 6, n 5. 1998. 3p. Disponível em: <http://www.emerald.com>. Acesso em: 16 abr. 2001.

SPARROW, P.R. **New employee behavious, work designs and forms of work organization wath is in store for the future of work?** Shefield: Jornal of Managerial Psychology, v 15, n 3, 12 p. Sheffield Uinversity, UK. 2000.

STACEY, T. **Toward standartization of information security: bs7799**. Sans Institute. 4p. 2000. Disponível em: <http://www.sans.org/infosecfaq/policy/standartization.htm>. Acesso em: 19 mar. 2001.

STEIL, A.V.; BARCIA, R.M. **Um modelo de prontidão organizacional para implantar o teletrabalho**. São Paulo: Revista de Administração da USP. 2000.

STURGEON , A. **Telework: treats, risks and solutions**. Ontário: Information Management & Computer Security, v 4, n 2. 1996.

TEIXEIRA JUNIOR, J.H. et al. **Redes de computadores – serviços, administração e segurança**. 1ª Ed. São Paulo: Ed. Makron Books. 1999.

TELECOMMUTING SECURITY GUIDE. US Department of Energy – Office of Information Management. 1997. Draft. 15p. Disponível em: <http://www.energy.state.or.us/telework/teleref.htm>. Acesso em: 1 abr. 2001.

TELMET. **Key issues covered in the deutsche telekom agreement**. 2001. Disponível em: <http://www.telmet.org/protocol%20report.htm>. Acesso em: 28 maio 2001.

THOMPSON, S.H.T.; VIVIEN, K.G.L. **Factorial dimensions and differential efects of gender on perceptions of teleworking**. Women in Management Review, v 13, n 7. 1998.

TOFFLER, A. **A terceira onda**. São Paulo: Ed. Record. 21ª Edição. 1995.

TROPE, A. **Organização virtual – impactos do teletrabalho nas organizações**. 1ª Ed. Rio de Janeiro: Ed. Qualitmark. 1999.

VERAS OLIVEIRA, M.M. **A Ergonomia e o trabalho no domicílio**. 100f. Dissertação (Mestrado em Engenharia da Produção) – Programa de Pós-Graduação em Engenharia de Produção – UFSC, Florianópolis. 1996.

YASIN, R**. Broadband access adds security – cable modems and adsl are "always on" does that mean they have to aways be a worry?** Internetweek, Manhasset. 2000.

WEISSENFLUSH, A. **Basic travel security**. 4p. 2000. Sans Institute. 3p. Disponível em: <http://www.sans.org/infosecfaq/ravel/trav_sec.htm>. Acesso em: 28 maio 2001.

WITHFORD, M. **Telecommuting on the superhighway**. Duluth: Hotel and Motel Management. 4p. 2000.

ZABROSKY, A.W. **The legal relity of virtual offices**. Consulting to Management, Burlingame. 2000.

Apêndice A

Questionário de Pesquisa

Segurança de Informação e Teletrabalho

INSTRUÇÕES

Prezado(a) colega

Participo do Programa de Pós-Graduação da Universidade Federal de Santa Catarina e, no momento, estou realizando minha dissertação de mestrado em Engenharia da Produção. A presente pesquisa tem como finalidade investigar algumas características sobre como as empresas estão tratando a questão da segurança da informação e seus teletrabalhadores.

*Por **teletrabalhadores**, entende-se aquelas pessoas, empregados da empresa ou prestadores de serviço, que empregando recursos de telecomunicações e informática, realizam suas atividades, ou parte delas, fora das instalações da empresa, seja em casa, com um microcomputador, seja como usuário móvel, com um notebook. Em todo caso, para ser caracterizado como teletrabalho, é necessário que o empregado tenha de interagir a distância com os recursos informacionais (a rede) da empresa.*

Você foi escolhido para fazer parte da amostra. Por essa razão solicito a gentileza de sua valiosa colaboração, preenchendo o questionário anexo, que contém uma série de itens relativos ao teletrabalho.

Por favor, responda a todas as questões, escolhendo a alternativa que melhor corresponda ao ambiente onde você realiza a maior parte de suas atividades diárias nesta organização.

Informo que as respostas serão tratadas de maneira confidencial e todos os resultados serão apresentados de forma a não permitir a sua identificação. O questionário não deve ser assinado ou identificado. Se preferir, remeta-o, preenchido, empregando uma conta de e-mail alternativo, de forma a impossibilitar sua identificação através do domínio da empresa.

Agradeço antecipadamente a sua indispensável colaboração. Peço ainda que a devolução seja feita até o dia 25 de julho.

Cesar de Souza Machado
E-mail: cesarm@cdigital.com.br
Home: www.cdigital.com.br/cesar.htm
Tel: (61) 447-7948

(1) Você trabalha na área de informática de sua organização?

( ) Sim ( ) Não

(2) A organização onde você trabalha tem atuação:

( ) Regional ( ) Nacional ( ) Internacional

(3) Em que estado do Brasil está localizada a organização em que você trabalha?

_____

(4 Quanto a natureza de sua organização, ela é uma empresa:

( ) Privada brasileira ( ) Multinacional ( ) Economia Mista ( ) Órgão público
( ) Associação, Sindicato, ONG ou assemelhada

(5) Com relação a experiência com teletrabalhadores, sua organização:

OBS: Se você marcar a primeira opção, passe para a questão 17.

( ) Não tem teletrabalhadores e nunca os teve
( ) Tem teletrabalhadores
( ) Já teve teletrabalhadores no passado mas não os tem mais
( ) Está estudando ou implantando um programa de teletrabalho

(6) Os teletrabalhadores, se houver, trabalham em que área (se for o caso, marque mais de uma opção)?

( ) Diretoria ( ) Gerência ( ) Comercial ( ) Informática ( ) Outras áreas:_____

(7) Os teletrabalhadores acessam a rede da empresa remotamente:

( ) Através de micros desktop instalados em suas residências
( ) Através de notebooks (usuário móvel)

(8) Como é feito o acesso do teletrabalhador à organização?

( ) Por linha telefônica discada ( ) Por Banda larga (Cable Modem, DSL ou outro)

(9) Com relação ao sistema do teletrabalhador, quais itens são fornecidos, pagos ou cedidos em comodato pela empresa (marque mais de um se for o caso):

( ) Microcomputador desktop (de mesa)
( ) Microcomputador notebook (portátil)
( ) Softwares
( ) Periféricos
( ) Acesso a Internet
( ) Nenhum dos itens acima especificados

(10) Com relação ao ambiente do teletrabalhador

( ) A empresa faz vistorias periódicas no local de trabalho do teletrabalhador
( ) A empresa faz vistorias periódicas no computador do teletrabalhador
( ) A empresa monitora por meio de ferramentas de gerenciamento (SNMP, por exemplo), o teletrabalhador
( ) Nenhuma dos itens acima especificados

(11) A política de segurança da empresa trata especificamente do teletrabalho?

( ) Sim ( ) Não

(12) O teletrabalhador é oficialmente informado acerca da política de segurança da empresa?

( ) Sim ( ) Não

(13) Os teletrabalhadores recebem treinamento com relação a segurança da informação?

( ) Sim ( ) Não

(14) Quanto a problemas de segurança da informação e teletrabalhadores, a organização:

( ) Nunca teve problemas de segurança com teletrabalhadores
( ) Já teve problemas de segurança com teletrabalhadores mas manteve o programa de teletrabalho
( ) Já teve problemas de segurança com teletrabalhadores e encerrou o programa o programa de teletrabalho
( ) Não implantou programa de teletrabalho diante dos riscos de segurança envolvidos
( ) Nunca teve problemas de segurança com teletrabalhadores mas encerrou o programa diante dos riscos envolvidos

(15) Quanto ao controle de acesso remoto dos teletrabalhadores:

( ) O teletrabalhador tem as mesmas permissões de acesso que um usuário da rede interna
( ) O teletrabalhador tem permissões de acesso mais restritas que um usuário da rede interna

(16) Quais ferramentas de segurança a empresa usa para atender as conexões dos teletrabalhadores (se for o caso, marque mais de uma opção):

( ) Firewall Corporativo (Na rede da empresa)
( ) Firewall pessoal (instalado no micro do teletrabalhador pela empresa)
( ) Anti-vírus (instalado na rede interna)
( ) Anti-vírus (instalado no micro do teletrabalhador pela empresa)
( ) IDS (Sistema de Detecção de Intrusos)
( ) Criptografia de arquivos
( ) Criptografia das comunicações (sem ser com o uso de VPN)
( ) VPN (Rede Privativa Virtual)
( ) PKI (Certificação digital)
( ) Call-Back (Retonro da ligação do teletrabalhador feita pelo servidor de acesso remoto)
( ) Servidor Radius (Servidor de comunicão/autenticação de usuários remotos)
( ) Biometria (Utilização de scanner para identificação da digital, irís ou outra variável corporal)
( ) Token Card (Cartão que contém a identificação digital do usuário capaz de autenticar seu logon)
( ) Logs e auditoria
( ) Outros:
_____

(17) Com relação ao suporte e manutenção do sistema (micro/softwares) do teletrabalhador:

( ) São prestados por funcionários da empresa
( ) São prestados por empresa credenciada pela organização
( ) São responsabilidade do teletrabalhador, sua organização não intervem

(18) Você conhece as normas de segurança da informação BS7799 e ISO17799?

( ) Não sei do que se trata ( ) Conheço superficialmente ( ) Conheço bem

(19) Qual é a relação de sua empresa com essas normas:?

( ) Formalmente, a empresa ainda não tomou conhecimento
( ) Está avaliando
( ) Está implantando
( ) Já implantou
( ) Já implantou e obteve a certificação correspondente

(20) Você tem interesse em avaliar uma metodologia para implementação da segurança da informação para teletrabalhadores?

( ) Sim ( ) Não

21) Relacione, se houver, os problemas de segurança da informação com relação a teletrabalhadores enfrentados por sua organização.

Anexo A

Controles da Norma ISO/DIS 17799

Referentes ao Teletrabalho

CONTROLES DA NORMA ISO/DIS 17799

REFERENTES A TELETRABALHO

9.8.2 Teletrabalho

O trabalho remoto utiliza tecnologia de comunicação para permitir que funcionários trabalhem remotamente a partir de uma localização física da sua organização. A proteção apropriada do local de trabalho remoto deve ser implantada para evitar, por exemplo, o roubo do equipamento e de informações, a divulgação não autorizada de informação, o acesso remoto não autorizado aos sistemas internos da organização ou o uso impróprio das facilidades. É importante que o trabalho remoto seja tanto autorizado quanto controlado pela gerência, e que sejam estabelecidos acordos adequados para esta forma de trabalho.

As organizações devem considerar o desenvolvimento de políticas, procedimentos e padrões para controlar as atividades do trabalho remoto. As organizações devem somente autorizar as atividades de trabalho remoto se existem controles e acordos de segurança apropriados e em vigor e que estejam em conformidade com a política de segurança da organização. Deve-se considerar o seguinte:

a) a segurança física existente no local do trabalho remoto, levando-se em conta a segurança física do prédio e o ambiente local;
b) o ambiente proposto de trabalho remoto;
c) os requisitos de segurança nas comunicações levam em conta a necessidade do acesso remoto para os sistemas internos da organização, a sensibilidade das informações que serão acessadas e trafegadas na linha de comunicação e a sensibilidade do sistema interno;
d) a ameaça de acesso não autorizado à informação ou recursos por outras pessoas que utilizam o local, por exemplo familiares e amigos.

Os controles e planejamentos que devem ser considerados incluem:

a) a provisão de equipamento e mobília apropriados às atividades de trabalho remoto;

b) uma definição do trabalho permitido, as horas de trabalho, a classificação da informação que pode ser manipulada e os sistemas internos e serviços que o funcionário é autorizado a acessar;
c) a provisão de equipamento de comunicação apropriado, incluindo metodos para acesso remoto seguro;
d) segurança física;
e) regras e orientações sobre o acesso de familiares e visitantes ao equipamento e a informação;
f) a provisão de suporte e manutenção de equipamento e software;
g) os procedimentos para cópias de segurança e continuidade do negócio;
h) auditoria e monitoração da segurança;
i) revogação de autoridade, direitos de acesso e devolução do equipamento quando as atividades de trabalho remoto cessarem.